Um caminho para a resiliência cibernética

Avaliação e proteção contra vulnerabilidades cibernéticas nos setores industriais

Dezembro de 2022

kpmg.com.br

Prefácio

A segurança cibernética está sendo testada de maneiras ousadas e sem precedentes conforme a frequência, a sofisticação e o impacto devastador dos ataques cibernéticos aumentam em todo o mundo. À medida que empresas de todos os setores correm em busca de soluções, as organizações industriais do setor de energia e recursos naturais estão enfrentando sua própria dura realidade ao reconhecer sua falta de preparação — e as consequências potencialmente catastróficas que elas enfrentam atualmente.

A ameaça de segurança cibernética às operações industriais evoluiu e aumentou rapidamente no último ano. O ataque de *ransomware* à Colonial Pipeline fez hackers derrubarem o maior oleoduto de combustível dos EUA, levando a uma grande escassez de combustível em maio de 2021 e forçando a empresa a pagar um pedido de resgate de US$ 4,4 milhões. De acordo com a empresa de segurança cibernética que respondeu ao incidente —considerado o maior ataque cibernético a um alvo de infraestrutura dos EUA até o momento —, o ataque foi resultado de uma única senha comprometida. Os hackers invadiram os sistemas de negócios da Colonial por meio de uma conta de rede privada virtual que dá acesso remoto à rede de computadores da empresa aos funcionários.[1]

Vários fatores, incluindo uma migração para o trabalho remoto para atividades de engenharia, linha de produção e manutenção — combinados com recursos digitais inadequados — contribuíram para a tendência alarmante em todo o setor. Além disso, a conscientização pública sobre a ameaça está crescendo após a violação da Colonial Pipeline e seu impacto disruptivo sobre empresas e consumidores. Os apelos públicos por ação ecoaram após o ataque.

Infelizmente, em meio à ameaça crescente e maior pressão pública por soluções, as organizações industriais permanecem em grande parte despreparadas para gerenciar e responder efetivamente às ameaças ferozes de hoje. As organizações podem estar enfrentando um paradoxo de escolha. Embora o setor de segurança cibernética esteja fornecendo diversas soluções para os mercados globais, muitas são relativamente novas e, algumas vezes, não testadas. Consequentemente, muitas organizações parecem confusas com as possíveis soluções e, portanto, estão postergando a ação sobre as inovações de segurança que inevitavelmente precisam fazer.

Esta publicação analisa o cenário atual de ameaças e apresenta orientações sobre como estar mais bem preparado para as ameaças destrutivas e potencialmente caras de hoje. A base da recomendação deste artigo é a análise de riscos de processos (PHA) cibernéticos como um conjunto de ferramentas para organizações industriais.

---

[1] William Turton and Kartikay Mehrotra, "*Hackers Breached Colonial Pipeline Using Compromised Password*," Bloomberg online, 4 de junho de 2021.

Sumário

Clique nos temas para obter mais informações.

Por que isso importa

Vários estudos sugerem que os líderes empresariais e governamentais reconhecem as ameaças cibernéticas industriais atuais, mas ainda não estão preparados para enfrentá-las. Embora os ataques cibernéticos sejam frequentemente transfronteiriços e a ameaça às empresas industriais seja global, as realidades geopolíticas e a concentração da atividade industrial em determinadas partes do mundo tornaram as ameaças mais acentuadas em alguns países.

Os números são impressionantes: Os ataques de *ransomware* em redes de tecnologia operacional (OT) aumentaram cinco vezes de 2018 a 2020. Desses ataques, as entidades de manufatura representaram mais de um terço dos ataques confirmados de *ransomware* a organizações industriais, seguidas pelas empresas de serviços públicos (*utilities*), que representaram 10%.[2]

E o custo global estimado desses ataques de *ransomware*? Também disparou e deve atingir US$ 20 bilhões em 2021 — em comparação com US$ 325 milhões em 2015.[3] A interrupção operacional resultante de ataques de *ransomware* em ambientes de OT registrou um aumento de 23 vezes. Em 2020, houve um aumento de 32% nos ataques de *ransomware* contra organizações de energia e utilidades.[4]

Certamente, somando-se às más notícias para o setor, está o fato de que os ataques de *ransomware* continuam crescendo em sofisticação. Além disso, os ataques têm como alvo cada vez mais ambientes de sistema de controle industrial (ICS), como petróleo e gás e manufatura.

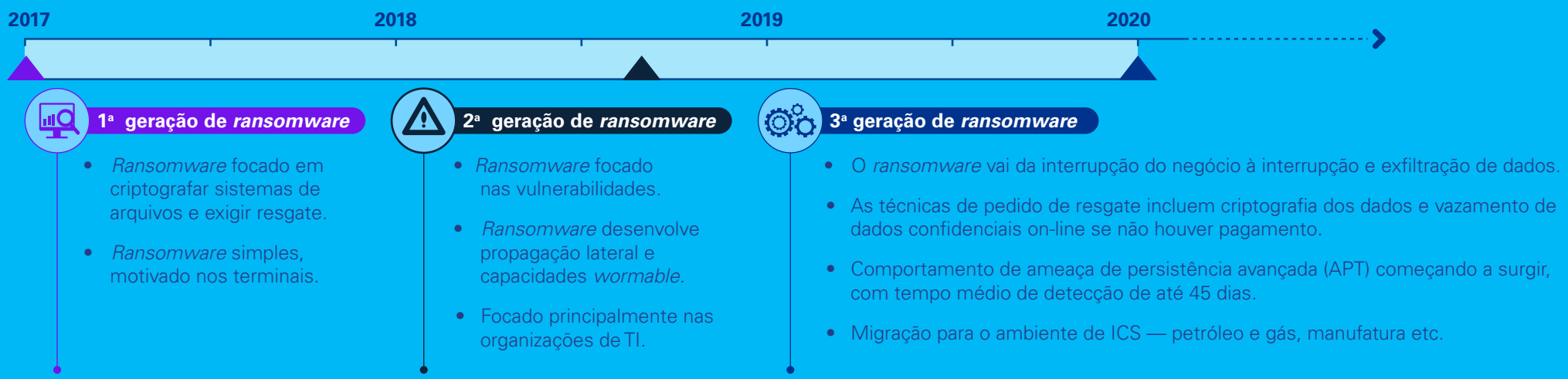
[2] *Ransomware in ICS Environments*, Dragos, dezembro de 2020.

[3] *Global ransomware damage costs predicted to exceed $265 billion by 2031*, *Cybersecurity Ventures*, 3 de junho de 2021.

[4] *Claroty Biannual ICS Risk & Vulnerability Report*: 1h 2020, Claroty, 2020.

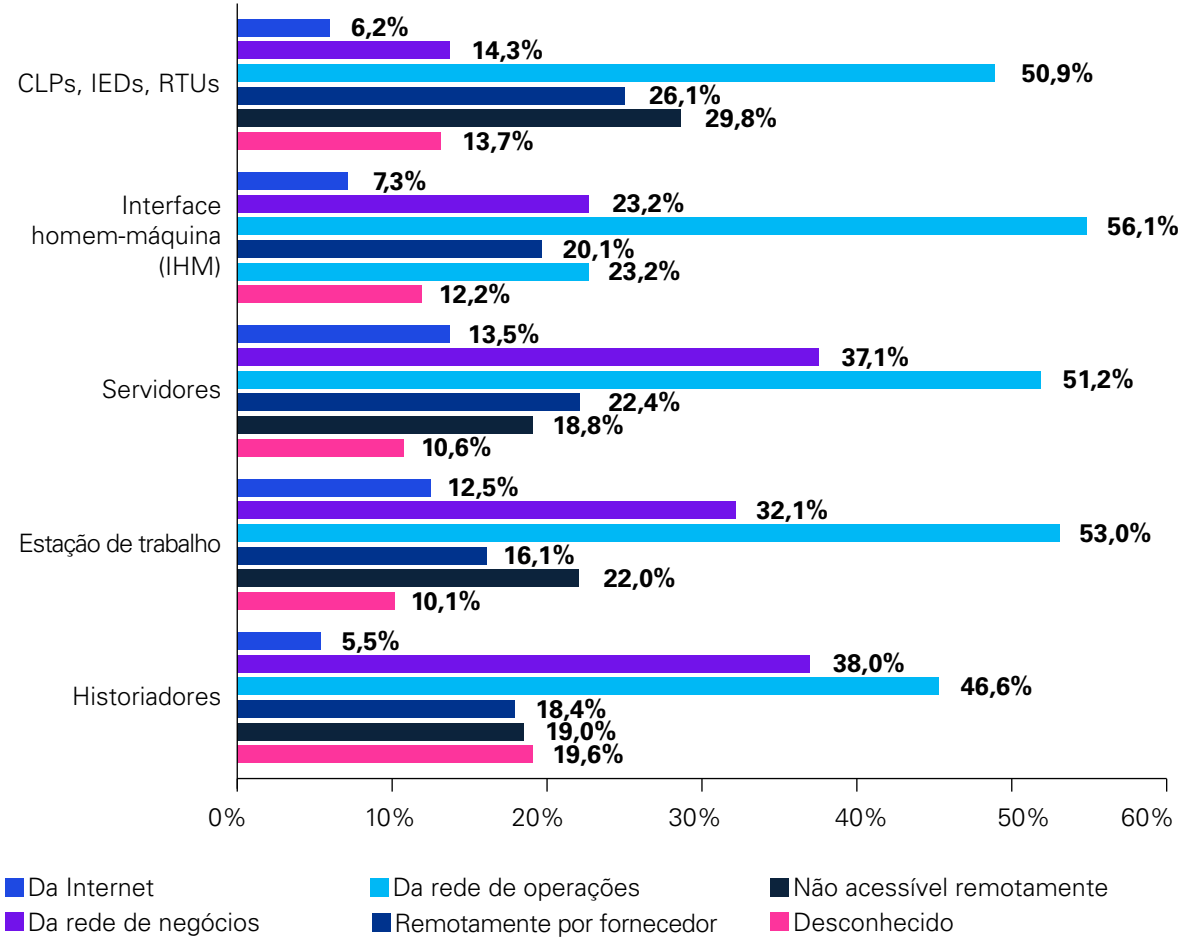
[5] *Securing a hyperconnected world*, KPMG International, 2021.

Figura 1: Ransomware em ascensão[5]



O estudo *Control System Cyber Security Survey* 2020 da KPMG e a (CS)²AI — *Control System Cyber Security Association International* — indicaram que 10% a 20% dos entrevistados não sabiam se algum componente/recurso indicado no gráfico abaixo estava acessível remotamente para seus negócios.

Figura 2: Componentes acessíveis remotamente[6]



[6] (CS)²AI-KPMG 2020 *Control System Cyber Security Survey, KPMG International*, 2020.

A evolução drástica do cenário atual de ameaças cibernéticas

Os agentes de ameaças continuam melhorando seu jogo.

Os criminosos cibernéticos estão mudando continuamente de tática em um esforço para evitar a detecção, aumentar suas perspectivas de sucesso e maximizar seus retornos em ataques de *ransomware*, incluindo:

- O uso crescente de sindicatos coesos de grupos do crime organizado.
- Reservar algum tempo para se familiarizar com as operações de vítimas potenciais.
- Ataques direcionados com mais precisão usando documentos legítimos que identificam vítimas em potencial para a entrega de *malware*.
- Comprar e vender acesso direto para ataques rápidos de *ransomware* em vez de realizar invasões avançadas que geralmente consomem mais tempo e são caras.

Os motivos dos ataques podem variar.

Como os invasores escolhem suas vítimas? Os motivos podem variar e muitas vezes são sustentados pela venda ilegal de senhas, ferramentas e técnicas de acesso a redes corporativas, que também está em ascensão. Além dos ganhos financeiros, os ataques de *ransomware* direcionados podem envolver diversos motivos, como fatores ideológicos ou políticos. No entanto, independentemente do motivo, medidas de segurança adequadas continuam sendo indispensáveis para gerenciar ataques com eficiência.

As cadeias de suprimentos estão enfrentando novas ameaças.

A melhora na higiene dos ecossistemas está empurrando as ameaças para a cadeia de suprimentos, transformando amigos em inimigos "desavisados". A interconexão global de negócios, a adoção mais ampla de medidas tradicionais de combate a ameaças cibernéticas e melhorias na segurança cibernética básica estão levando os agentes de ameaças a buscar novas abordagens que visam cada vez mais as cadeias de suprimentos — incluindo *software, hardware* e serviços em nuvem.

As vulnerabilidades da infraestrutura de OT/ICS exigem soluções caras.

A descoberta, nos últimos anos, de vulnerabilidades em controladores lógicos programáveis (CLPs), interface homem-máquina (IHM), historiadores ou estações de trabalho de engenharia representam um alto risco para as organizações. Em alguns casos, nos quais as vulnerabilidades na infraestrutura crítica são focadas, as operações podem ser afetadas fisicamente — causando riscos de segurança e até mesmo levando à perda de vidas.

Na mira da geopolítica.

Conforme novas ameaças surgem, as empresas podem enfrentar o impacto negativo das tensões geopolíticas e das ameaças cibernéticas dos estados-nação. Esses criminosos cibernéticos podem tirar vantagem de novos recursos à medida que novas tecnologias possibilitam táticas, técnicas e procedimentos (TTPs) mais sofisticados, focados nos ambientes de OT/ICS.[7]

[7] *Security magazine, Five factors influencing the cyber security threat landscape*, 2019.

Resiliência cibernética

De acordo com o Departamento de Segurança Interna dos EUA, a resiliência cibernética visa assegurar que os sistemas de negócios continuem desempenhando funções de missão crítica durante um ataque cibernético. A resiliência cibernética é particularmente importante para um subconjunto de infraestruturas críticas conhecidas como setores fundamentais ou infraestruturas estratégicas.[8] E não são apenas os EUA que dão ênfase adicional à resiliência cibernética para a infraestrutura crítica.

A Diretiva NIS de 2016 da UE está em constante evolução para aprimorar as capacidades cibernéticas entre as infraestruturas críticas. A UE também está se preparando para lançar a Lei de Resiliência Operacional Digital (DORA), que visa reforçar a resiliência cibernética para serviços financeiros entre os setores vitais mostrados na Figura 3.

Além disso, a Autoridade Nacional de Segurança Cibernética da Arábia Saudita ordenou que todos os reguladores setoriais desenvolvessem estruturas específicas do setor para apoiar a estratégia e regulamentação de segurança cibernética do país.

Distinguir a resiliência cibernética da segurança cibernética

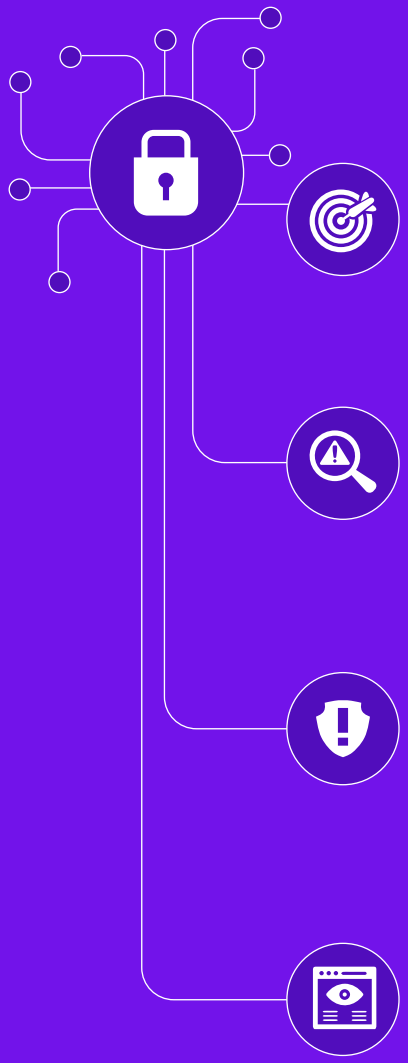
Um ponto-chave que diferencia a resiliência cibernética da segurança cibernética é que os recursos de resiliência cibernética continuam funcionando mesmo depois que um adversário penetrou no perímetro de segurança de uma rede para comprometer os ativos cibernéticos. Mesmo nas etapas posteriores da *cyber-kill chain*, a resiliência cibernética pode ajudar a impedir que os adversários coletem informações, extraiam dados ou assumam o controle de sistemas essenciais à missão.

Um programa de resiliência cibernética personalizado pode servir após o comprometimento, juntamente com um manual projetado para atingir resultados de resiliência cibernética com base em uma perspectiva de engenharia de sistemas nos processos de ciclo de vida de sistemas. A natureza personalizável dos esforços de engenharia e dos processos de ciclo de vida garante que os sistemas que aplicam os princípios de projeto de resiliência cibernética sejam suficientes para proteger as partes interessadas da perda de ativos importantes e das consequências econômicas e de segurança nacional associadas.

A engenharia de sistemas com resiliência cibernética para combater o cenário de ameaças em evolução atual envolve as seguintes características que devem ser consideradas ao projetar novos sistemas ou melhorar os existentes.

Figura 3: Setores vitais

[8] *US Department of Homeland Security, Cyber Resilience and Response* (2018)



Características para elaborar sistemas ciber-resilientes

Foco na missão e nos objetivos do negócio.

Isso envolve a capacidade de apoiar a continuidade do negócio, apesar dele estar comprometido. Em alguns casos, os componentes do sistema que são menos críticos para a missão ou efetividade do negócio podem ser sacrificados para conter um ataque cibernético e ajudar a maximizar os objetivos da missão.

Concentre-se nos efeitos das ameaças persistentes avançadas (APT).

Os recursos, a discrição e a capacidade de adaptação de uma APT a tornam uma ameaça perigosa. Ao se concentrar nas atividades de APT e seus efeitos potenciais, os engenheiros podem projetar sistemas que antecipam, resistem, se recuperam e se adaptam a um conjunto amplo e diversificado de condições e tensões adversas.

Suponha que um adversário possa comprometer ou violar o sistema ou a organização.

Essa crença é fundamental para o projeto da resiliência cibernética. Essa premissa reconhece que os sistemas modernos são entidades grandes e complexas que provavelmente sempre terão pontos fracos e falhas que os invasores podem visar e explorar.

Suponha que o adversário provavelmente manterá uma presença prolongada.

Pode ser difícil determinar que uma ameaça furtiva foi erradicada. A APT pode se adaptar a táticas de mitigação ou interpretação que antes eram eficazes contra a ameaça. Em algumas situações, o melhor resultado pode ser conter a presença de um adversário o suficiente para que a organização possa atingir seus objetivos de missão primária antes de perder as capacidades críticas dos sistemas.

O valor da resiliência cibernética no nível corporativo

Em função da complexidade inerente e da natureza dinâmica das técnicas de resiliência cibernética, implementar e manter, inicialmente, a resiliência cibernética apropriada pode custar mais do que implementar e manter as medidas tradicionais de segurança cibernética. Entretanto, apesar dos seus custos mais altos de implementação e manutenção, a resiliência cibernética pode custar à empresa menos do que as medidas tradicionais de segurança cibernética quando avaliada com base no custo ao longo do ciclo de vida, dada a capacidade dos recursos de resiliência cibernética de resistir a ataques e, em última análise, evitar o tempo de inatividade dispendioso da empresa e a perda de receitas.

Um ataque cibernético sofisticado projetado para parar uma empresa de infraestrutura crítica pode paralisá-la por várias semanas, em vez de apenas vários dias com ataques menos sofisticados. Calcular a perda potencial estimada de receita e clientes, em comparação com o custo de implementação de princípios e técnicas de projeto de resiliência cibernética, é o que determina se a resiliência cibernética oferece um bom custo-benefício para a empresa.

Valor da resiliência cibernética no nível social

Mesmo que um investimento em resiliência cibernética não gere um benefício econômico líquido no âmbito da empresa, ele ainda pode gerar um benefício econômico no nível social. As empresas de infraestrutura crítica que sabem que o fechamento de sua empresa teria efeitos em cascata em toda a região em que atuam devem poder apresentar esse caso aos seus governos. Quando uma empresa não consegue preparar o caso de negócios para a sua própria resiliência cibernética, mas reconhece o quanto outras empresas são dependentes dela, pode preparar o caso de negócios no nível da sociedade regional.

Dois exemplos que demonstram a natureza mutável dos ataques cibernéticos no setor industrial

Ataque a oleoduto dos Estados Unidos

Em maio de 2021, os EUA sofreram uma grande violação de segurança cibernética quando o oleoduto Texas-Nova York da Colonial Pipeline, o maior do país, foi forçado a parar durante um ataque de *ransomware*. Conforme mencionado, a empresa teve que pagar US$ 4,4 milhões de resgate aos hackers. O incidente que afetou milhões de consumidores e empresas é considerado uma das operações de resgate digital mais disruptivas e caras até hoje nos EUA e provocou um intenso escrutínio em relação à vulnerabilidade da infraestrutura atual de energia do país.

Vazamento de dados em gigante global de energia

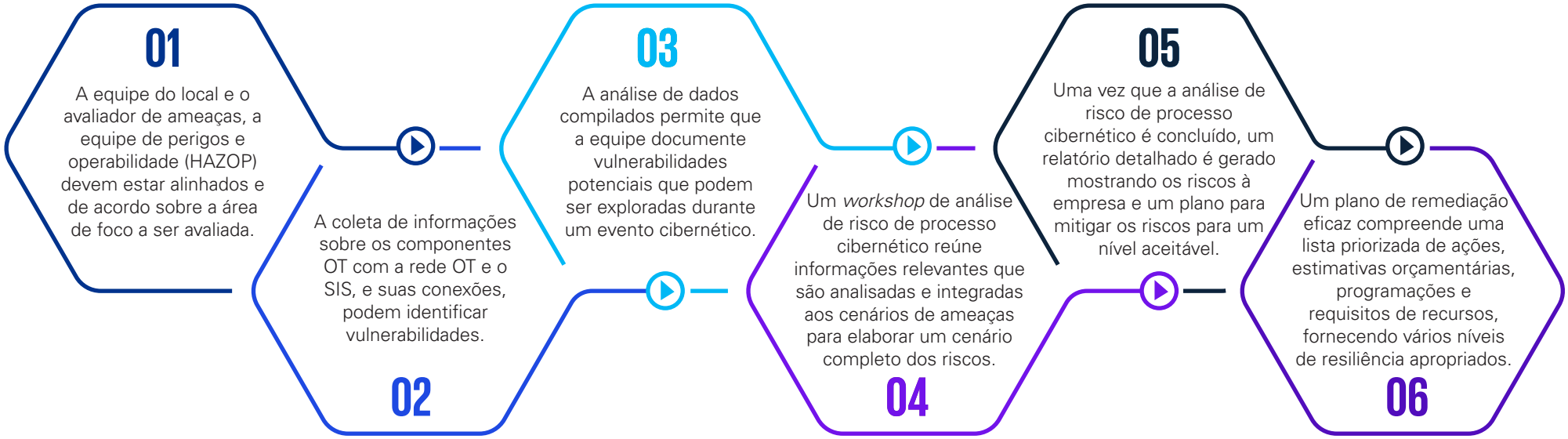
Em meados de 2021, uma empresa global de energia enfrentou um vazamento de dados envolvendo um de seus subcontratados. Um terabyte de dados de negócios foi mantido por invasores na tentativa de extorquir fundos da empresa. Esses incidentes destacam novamente a importância fundamental de investir em segurança cibernética moderna em meio ao aumento contínuo de ataques cibernéticos.

O método de PHA

Facilitando uma análise de riscos de processos cibernéticos (PHA)

Uma análise de risco de processo cibernético é uma metodologia orientada à segurança para realizar uma avaliação de riscos de segurança cibernética para um ICS ou sistema instrumentado de segurança (SIS). Ela é normalmente realizada em fases, sendo escalável e podendo ser aplicada a sistemas individuais ou instalações ou empresas inteiras.

As seis fases para uma análise de risco de processo cibernético



Automação ampliada

A segurança cibernética não deve ser vista simplesmente como proteção para ativos antigos ou vulneráveis.

Certamente pode ser difícil adaptar a segurança cibernética para sistemas como redes elétricas em meio a limitações para atualizá-los, corrigi-los ou até mesmo mantê-los. No entanto, para sistemas industriais mais novos que integram automação, os protocolos de segurança cibernética são tão importantes, se não mais atualmente.

Conforme os sistemas de manufatura automatizados são introduzidos e os sistemas de TI e OT convergem, as organizações devem incorporar a segurança cibernética nas funções principais.

Modelos de maturidade para o desenvolvimento futuro de sistemas de manufatura automatizados com funcionalidade de TI estão surgindo continuamente. Um modelo bem estabelecido, definido há alguns anos na Alemanha e aplicável atualmente, descreve cinco etapas para uma nova geração de sistemas de automação de ação e otimização automática, que exigem um alto grau de autonomia (consulte a figura 4).[9] As três primeiras etapas envolvem a aquisição de dados e sua análise sistemática.

A automação de sistemas industriais e a convergência de TI/OT significa que os sistemas industriais — antes isolados e seguros — estão se tornando cada vez mais integrados às redes corporativas, algumas vezes em plataformas comerciais de prateleira. Essa conectividade pode criar benefícios potenciais, como análise inteligente, manutenção preditiva e monitoramento remoto.

Mas ela também expõe o sistema de controle industrial (ICS), sistemas de controle de processos e outras tecnologias operacionais a ataques de *malware*, hacktivismo, sabotagem de funcionários e outros riscos de segurança que anteriormente afetavam apenas as informações corporativas de TI.

Figura 4: Cinco etapas para sistemas de automação futuros

[9] Michael Weyrich, *Towards future Automation Systems – Cyber physical, intelligent, flexible and efficient*, 2018

Conforme as linhas entre TI e OT se confundem, um PHA cibernética pode ajudar a fornecer acesso adequado aos dados de controle e produção, evitando eventos de segurança cibernética que podem causar paralisações dispendiosas, ameaças graves à segurança e interrupções significativas de processos.

Estrutura regulatória

Conforme a implementação de sistemas cibernéticos cresce em todos os setores, é fundamental definir normas de segurança e medidas regulatórias que possam ajudar a garantir a proteção de dados e sistemas. O método de gerenciamento de segurança de processos foi promulgado em 1992 e é um programa abrangente que evita a liberação de materiais perigosos, normalmente sustentado pelo compromisso da administração, e inclui 14 elementos relacionados, como envolvimento de funcionários, treinamento, análise de risco de processos e informações de segurança de processos. Consulte a figura 5.

As organizações já começaram a tomar medidas regulatórias para se proteger contra ataques. Por exemplo, a norma de segurança funcional 61511 da Comissão Eletrotécnica Internacional (IEC) agora exige uma avaliação de risco de segurança do SIS. O relatório atualizado resume o procedimento de avaliação de risco chamado de análise de riscos de processos (PHA) cibernético. O *link* para a PHA aqui é um passo na avaliação de risco para, em primeiro lugar, analisar os achados da PHA para identificar as consequências do pior caso de saúde, segurança e meio ambiente (SS&MA) para o ativo e, em segundo lugar, identificar quaisquer cenários de perigo.

Outro exemplo vem da Associação dos Usuários de Tecnologia de Automação em Indústrias de Processo (NAMUR), que já publicou uma planilha (NA 163) intitulada "*Security assessment of SIS*" (Avaliação da segurança do SIS). Aqui, a metodologia de análise de riscos de processos (PHA) cibernéticos pode avaliar os riscos relacionados aos fatores de escalação de segurança cibernética identificados e as mitigações recomendadas para ajudar a reduzir os riscos a um certo nível.

Figura 5: Ilustração de padrões de saúde e segurança ocupacional[10]

[10] Departamento de Trabalho dos EUA, Administração de Segurança e Saúde Ocupacional, 1910.119 - Gerenciamento de segurança de processo de produtos químicos altamente perigosos.

Ao criar uma ponte entre os métodos de análise de riscos de processos (PHA) e os métodos de avaliação de risco de segurança cibernética, os sistemas de segurança podem se tornar mais robustos contra os ataques.

Algumas empresas globais de energia vêm implementando métodos há muito tempo para avaliar riscos e aumentar a segurança. Esses esforços incluem o uso de matrizes de avaliação de risco que consideram a consequência do risco para pessoas, ativos, comunidade e meio ambiente, além de modelos gravata borboleta (*bow-tie*) para visualizar os diversos elementos dos cenários de risco. Uma ferramenta de risco de análise de riscos de processos (PHA) cibernéticos pode ajudar a facilitar um exercício holístico de PHA cibernéticos. Isso inclui o seguinte:

- Uma revisão da documentação existente;
- Uma lista de todos os ativos cibernéticos;
- Análises do local;
- Coleta e revisão de análises de PHA anteriores; e posteriores;
- Uma lista de todos os tipos de ativos cibernéticos utilizados em cada processo específico ou unidade de utilidade sempre que houver riscos financeiros, ambientais ou de segurança de processos diferentes.

Para que um ataque cibernético ocorra, tanto a iniciação quanto a proteção devem ser passíveis de invasão. Ao tornar um dos dois não "hackeáveis", o risco pode ser reduzido. E tornando ambos não "hackeáveis", o risco pode ser eliminado. Embora avaliar a vulnerabilidade seja crucial, isso não é suficiente para se proteger contra ataques cibernéticos. Outro fator essencial a considerar é entender vários tipos de ameaças cibernéticas. O treinamento da equipe em conscientização sobre segurança cibernética é uma parte essencial do processo, pois cria um entendimento mais profundo das ameaças e salvaguardas cibernéticas.

É fundamental realizar uma análise de caminho de rede e validar a segmentação de rede e os isolamentos funcionais. A arquitetura do sistema de comunicação deve sempre ser verificada em relação ao nível de segurança exigido para a zona com a qual interage.

Figura 6: Exemplo de topologia de uma linha

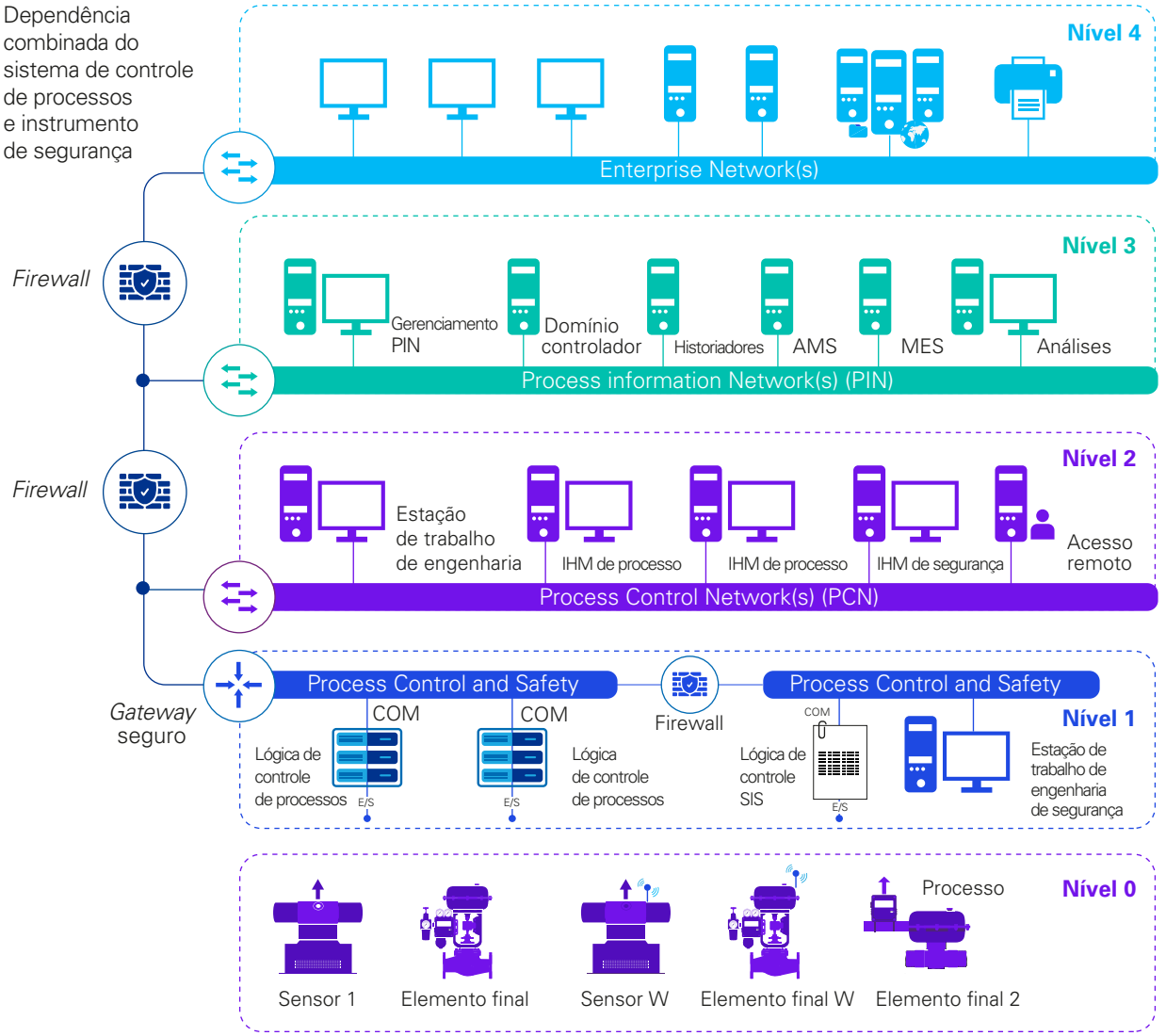
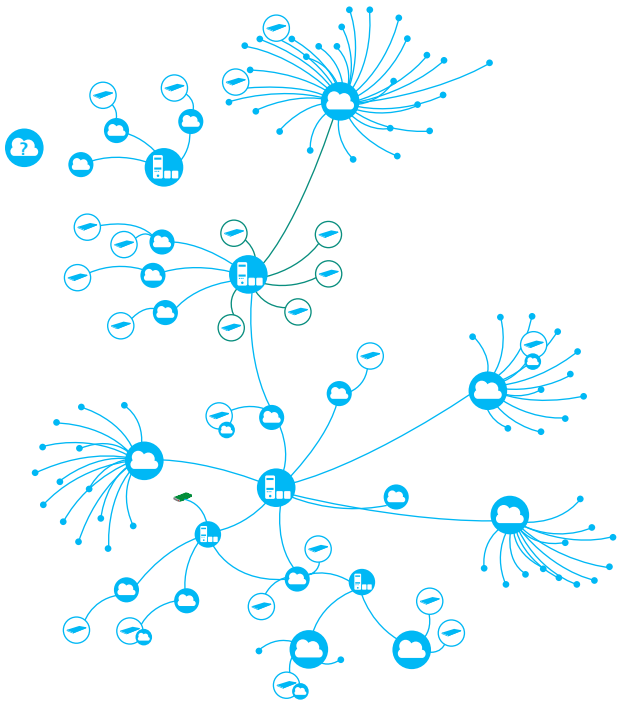


Figura 7: Saída de topologias de rede demonstrando interconexões e exemplo de análise de caminhos.



Resultados para uma análise de riscos de processos (PHA) cibernéticos

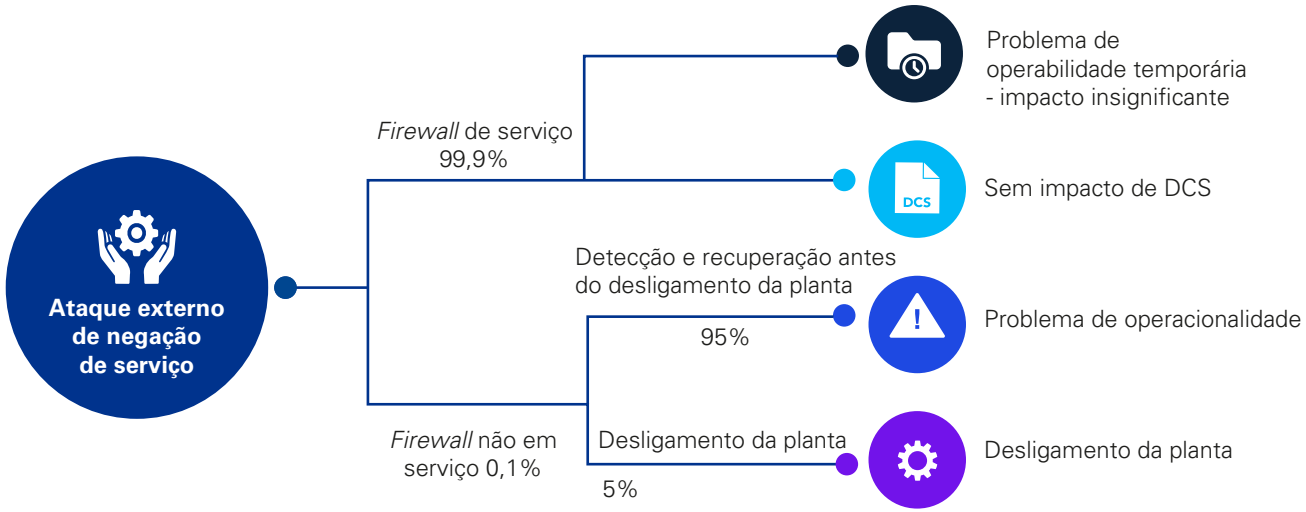
O resultado da análise deve identificar possíveis perigos e vulnerabilidades e, ao mesmo tempo, fornecer temas para discussão dos riscos que facilitam recomendações práticas para implementação. Embora o cenário de ameaças esteja mudando continuamente, existem classificações gerais dos agentes ou fontes de ameaças para uma organização considerar:

Agentes/fontes de ameaças potenciais

1. Ataque externo — técnico
2. Ataque interno — não técnico
3. Uso indevido e abusos internos
4. Acesso não autorizado
5. Comprometimento de informações (*Logic Mod*)
6. Mau funcionamento do sistema
7. Interrupção de processo
8. Interrupção do sistema de segurança
9. Erro humano
10. Efeito imprevisto de mudanças

A Figura 8 ilustra como isso funciona na prática, considerando o risco residual do sistema de controle distribuído (DCS) e a implementação de contramedidas.

Figura 8: Risco residual de DCS e implementação de contramedidas.



Benefícios potenciais de uma análise de riscos de processos (PHA) cibernéticos

Conforme as ameaças e os impactos cibernéticos aumentam entre as empresas industriais, os benefícios potenciais da análise de riscos de processos (PHA) cibernéticos são numerosos. O mais óbvio é a segurança do sistema. Uma metodologia de análise de riscos de processos (PHA) cibernéticos, quando implementada corretamente, pode incutir práticas em todo o sistema industrial que podem ajudar a prevenir a maioria dos ataques cibernéticos.

Além do benefício obvio esperado da segurança, a análise de riscos de processos (PHA) cibernéticos também pode beneficiar as práticas de negócios mais amplas de uma organização. A aplicação de uma metodologia de análise de riscos de processos (PHA) cibernéticos documenta os processos de negócios de uma organização e exige a criação de políticas, procedimentos, normas e controles integrados de segurança da informação usados em uma organização.

Benefícios comerciais potenciais da análise de riscos de processos (PHA) cibernéticos

A seguir são apresentados possíveis benefícios comerciais da análise de riscos de processos (PHA) cibernéticos:

Articulação da estratégia de segurança da informação claramente definida com base nos objetivos da organização e da unidade de negócio.

Definição do conhecimento de engenharia com controles de segurança alinhados com base no risco e nos objetivos do negócio.

Pessoal efetivo confiante em virtude das funções e responsabilidades estabelecidas.

Identificação de causas e impactos do sistema interconectado, facilitando o gerenciamento de risco e vulnerabilidades.

Resposta cibernética direcionada e priorizada, e gerenciamento de incidentes.

O SecOps (Segurança e Operações) definiu métricas, relatórios e requisitos.

Figura 9: Segurança cibernética e otimização de custos via Operações de Segurança (SecOps)

Estudo de caso

Implementando uma análise de riscos de processos (PHA) cibernéticos para uma organização industrial

O cliente precisava padronizar seus processos em um ambiente heterogêneo de sistemas e vários fornecedores, levando todos ao mesmo nível de segurança operacional.

Desafios do cliente

Nenhum CSMS em vigor

Ausência de um sistema de gerenciamento de segurança cibernética (CSMS) definido para o ambiente de manufatura.

Processos desconectados em todas as operações

Presença de várias plantas operadas por várias partes interessadas utilizando processos e sistemas separados.

Nenhuma rede de referência modelo

Ausência de um diagrama de rede padrão e modelo de referência de acordo com o modelo *Purdue* e com as diretrizes ISA 62443 para suas diferentes plantas.

A resposta

Relatório de avaliação de *gaps* e entrevistas

Isso é fundamental para entender a postura de segurança atual de acordo com as diretrizes da International Society of Automation (ISA). Criação subsequente de uma estrutura de segurança padronizada e comum, e um programa de CSMS padrão para toda a organização.

Projeto de painéis de monitoramento

Possibilitar que a alta administração represente o status atual versus o *status* de segurança desejado do ambiente de ICS para entender o nível de exposição.

Projeto do *roadmap* para implementar as iniciativas de segurança identificadas

Possibilitando que o cliente rastreie e implemente os *roadmaps* desejados em todo o ambiente de ICS em termos de prioridade.

Avaliação técnica de segurança de CPLs e aplicativos de controle de supervisão e aquisição de dados (SCADA)

Avaliação da postura geral de segurança técnica de dispositivos embarcados e CLPs na planta.

Os cenários de ameaças e os casos de ameaças de lógica de negócios projetados para realizar a avaliação forneceram ao cliente uma visão da superfície de ataques existente e possíveis áreas de comprometimento em caso de ataque.

Análise de risco de processo com base na análise de riscos de processos (PHA) cibernéticos

Revisamos os *gaps* de segurança cibernética com base no HAZOP e nos procedimentos de análise de camadas de proteção (LOPA) e mapeamos a avaliação para as categorias de risco definidas em Saúde e Segurança, Meio Ambiente, Finanças e Operações, atribuindo assim o risco geral aos desvio.

Relatório de avaliação dos níveis de segurança do sistema

Níveis de segurança avaliados para cada sistema em uma zona e conduíte na rede de ICS.

Desenvolvimento de um relatório de arquitetura de rede

Zonas projetadas e conduítes para duas plantas com dois tipos diferentes de rede de ICS. Os *gaps* identificados foram apresentados aos fornecedores da planta para melhorar o projeto geral da arquitetura de segurança da planta.

Como os profissionais da KPMG podem ajudar

As firmas da KPMG podem ajudá-lo a criar um mundo digital resiliente e confiável — mesmo diante das ameaças em mudança. Os profissionais de segurança cibernética da KPMG podem oferecer uma visão multidisciplinar do risco, ajudando-o a implementar a segurança em toda a sua organização, para que você possa antecipar o futuro, mover- se com mais rapidez e obter uma vantagem com tecnologia segura e confiável.

Não importa onde você esteja na sua jornada de segurança cibernética, as firmas da KPMG têm experiência em todo o espectro — da sala do conselho ao data center. Além de avaliar sua segurança cibernética e alinhá-la às suas prioridades de negócios, os profissionais KPMG podem ajudá-lo a desenvolver soluções avançadas, implementá- las, assessorá-lo no monitoramento dos riscos contínuos e ajudá-lo a responder a incidentes cibernéticos com eficácia.

As firmas da KPMG oferecem uma combinação incomum de especialização tecnológica, profundo conhecimento de negócios e profissionais criativos que são apaixonados em ajudá-lo a proteger e construir o seu negócio. Os profissionais da KPMG podem ajudar a criar um mundo digital confiável, para que você possa ultrapassar os limites do que é possível.

Colaboradores

Ton Diemont
Diretor sênior de Cyber Security & Privacy da KPMG na Arábia Saudita

Hossain Alshedoki
Diretor de Cyber Security & Privacy em TI/OT na área de Energia da KPMG na Arábia Saudita

David Ferbrache
Sócio-líder de Cyber Futures da KPMG no Reino Unido

Ronald Heil
Sócio-líder global de Cyber Security para a área de Energia e colíder nacional de Cyber Security da KPMG na Holanda

Jason Haward-Grau
Diretor de Cyber Security da KPMG nos EUA

Walter Risi
Sócio-líder global de Cyber Security em IoT da KPMG na Argentina

Dani Michaux
Sócia-líder de Cyber Security da KPMG na Irlanda e na região EMA (Europa, Oriente Médio e África

Fale com o nosso time

Leandro Augusto
Sócio-líder de Cyber Security & Privacy da KPMG no Brasil e na América do Sul
lantonio@kpmg.com.br

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

A prestação de todos ou de alguns dos serviços aqui descritos pode não ser permitida para clientes de auditoria da KPMG e suas afiliadas ou entidades relacionadas.

kpmg.com.br

/kpmgbrasil