KPMG

Trazendo a análise de riscos de processos cibernéticos para a era digital

Ampliando a verificação dos perigos dos riscos cibernéticos

Por: Hossain Alshedoki e Tim Johnson

A análise de risco de processos (*Process Hazard Analysis* - PHA, na sigla em inglês) é um recurso já utilizado nas plantas de petróleo e gás e industriais. Essa avaliação realiza revisões e remediações de hardware nas operações desses processos. Com base na metodologia da OHSA 1910.119, a PHA se baseia em 14 elementos interrelacionados para criar um programa abrangente e evitar a liberação de materiais perigosos[1].

Mas à medida que o hardware nas redes das indústrias se torna cada vez mais preparado com o avanço da tecnologia — com componentes de controle comunicando-se uns com os outros, em um domínio de Sistema de Controle Industrial (*Industrial Control System* - ICS, na sigla em inglês) ou Tecnologia Operacional (*Operational Technology* - OT) —, novos riscos surgem, exigindo novos níveis de PHA.

Esses componentes não são mais itens autônomos que existem de forma isolada, desconectados das outras partes do domínio ICS ou da rede de tecnologia da informação (TI). A necessidade de interação do ICS/OT com a TI está produzindo uma convergência crescente, expandindo caminhos e pontos principais por meio de processos críticos de controle de processo.

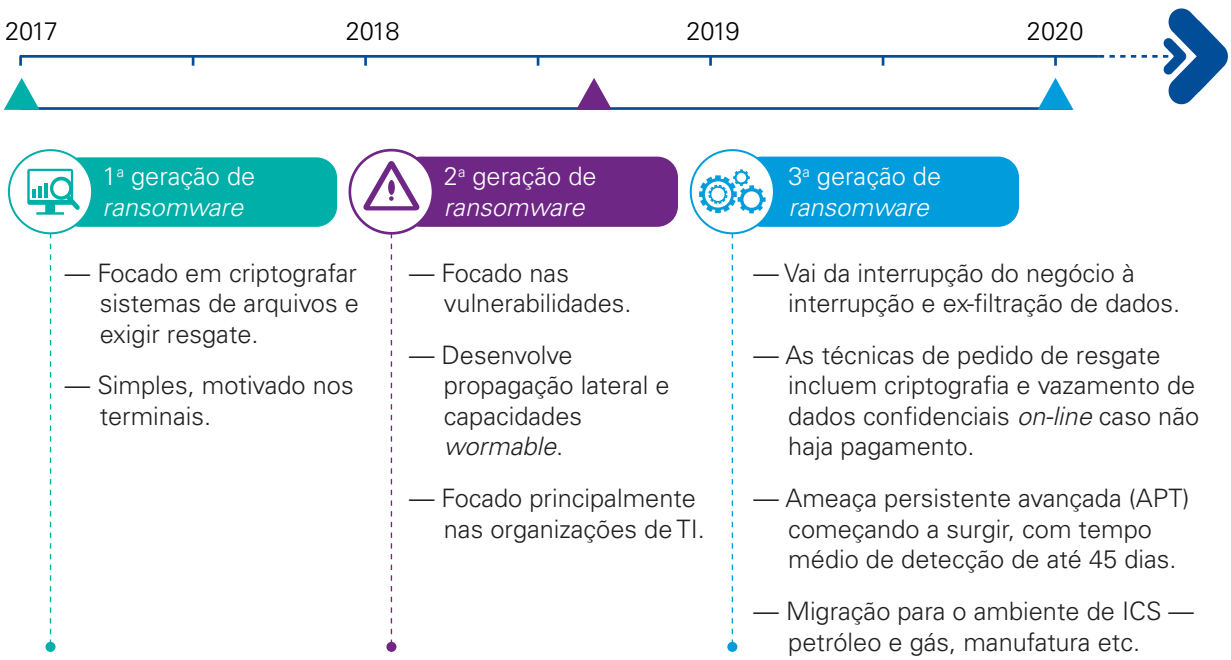
Existe uma interseção crescente entre sistemas de segurança e de controle de processo, resultando em novas possibilidades de ataque que podem ser exploradas pelos invasores cibernéticos.

Esse problema está se tornando uma realidade. Os ataques de *ransomware* nas redes de OT têm se multiplicado: eles aumentaram cinco vezes de 2018 a 2020. Desses ataques, as indústrias receberam mais de um terço dos ataques confirmados de *ransomware*, seguidos por empresas de serviços públicos, com 10%[2] dos ataques sofridos.

O custo global estimado dos ataques de *ransomware* disparou, e prevê-se que chegará a US$ 20 bilhões em 2021 – bem acima do custo de US$ 325 milhões em 2015[3]. As interrupções operacionais devidas a *ransomwares* em ambientes de OT aumentaram 23 vezes. Em 2020, houve um aumento de 32% nesse tipo de ataque em organizações de energia e serviços públicos[4].

Com o tempo, os ataques de *ransomware* se tornaram mais sofisticados para atingir seus objetivos por diferentes métodos. Além disso, esse tipo de ameaça tem visado os ambientes de ICS de maneira crescente, como em empresas de petróleo e gás e indústrias de manufatura.

Ataques de *ransomware* em alta



[1] US DEPARTMENT OF LABOR, OCCUPATIONAL SAFETY AND HEALTH ADMINISTRATION. *Process safety management of highly hazardous chemicals*. 1910.119

[2] DRAGOS. *Ransomware in ICS Environments*. 2020.

[3] CYBERSECURITY VENTURES. *Global ransomware damage costs predicted to exceed* $265 *billion by* 2031. 2021.

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

Cenário de crescentes ameaças

Os ataques de *ransomware* são apenas algumas das características de um cenário de ameaças complexo e cada vez mais agressivo, contra o qual as organizações precisam se proteger. A seguir, apresentamos outros pontos de atenção:

As ameças estão evoluindo

Os criminosos cibernéticos estão se adaptando, diversificando-se e se comportando mais como usuários legítimos. As operações de ataque estão mudando de tática para diminuir os riscos de detecção e de transtornos.

Os invasores tentam maximizar o retorno de seus ataques por meio de estratégias diversas, tais como: diversificação de alianças para operar dentro de locais com os quais os usuários tenham relacionamento, como sindicatos de funcionários; benefícios obtidos pela disponibilidade cada vez maior de informações do ICS para promover ataques; precisão maior dos alvos com o uso de documentos autênticos para identificar prováveis vítimas antes de instalar *malwares*; compra e venda de acesso direto a redes para instalar *ransomwares*, ao invés de realizar invasões avançadas.

Ransomware direcionado

Há uma gama complexa de motivos para os ataques de *ransomware* direcionados. Embora a motivação por trás de um ataque possa parecer financeira, podem existir motivos diferentes – uma combinação de fatores financeiros, ideológicos ou políticos. Independentemente do motivo, esses ataques têm o potencial de impactar a disponibilidade do ICS/OT. Enquanto as ameaças existirem, as organizações deverão tomar providências para se preparar, prevenir, detectar, responder e deter um ataque de *ransomware*.

Ameaças à cadeia de suprimentos

A melhoria na limpeza dos ecossistemas está levando as ameaças para a cadeia de suprimentos. A interconectividade global das empresas, a maior adoção de medidas contra as ameaças cibernéticas pela indústria tradicional e o aprimoramento da segurança cibernética parecem levar os criminosos cibernéticos a buscar novos caminhos para atacar as organizações, como as cadeias de suprimentos – inclusive as de software, hardware e serviços em nuvem.

A vida após o desastre

As vulnerabilidades na infraestrutura do ICS/OT exigem soluções ajustadas e direcionadas para evitar o impacto na disponibilidade de produtos e serviços. A descoberta de fragilidades no *hardware* de controle de processos proprietário, como controladores lógicos programáveis (*programmable logic controllers* – PLCs), software e hardware comercial para interfaces homem-máquina (*human machine interfaces* - HMIs), estações de trabalho de engenharia e sistemas de suporte ao ICS, como os historiadores, têm um impacto na disponibilidade do sistema e aumentam o risco para as organizações, o que poderia levar à perda de vidas.

Comprometendo a geopolítica

À medida que novas ameaças surgem da desinformação e da evolução tecnológica, as empresas globais podem se encontrar no alvo dos ataques enquanto persistirem as tensões geopolíticas. Os criminosos cibernéticos podem não apenas manter os níveis de atividade atuais, como também tirar vantagem de novos recursos, conforme novas tecnologias possibilitam táticas, técnicas e procedimentos (TTPs) mais sofisticados e focados nos ambientes de ICS/OT[6].

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

[6] SECURITY MAGAZINE. *Five factors influencing the cyber security threat landscape.* 2019

Fortalecendo as defesas por meio de PHA cibernética

Em decorrência desses fatores, é necessário expandir a PHA tradicional para proteger o controle de processos realizados no domínio ICS/OT. Essa necessidade é mais crítica porque a comunicação do sistema de segurança está sendo integrada ao domínio ICS/OT conforme ele se torna mais digitalizado e conectado. Se o sistema de segurança interconectado for comprometido, a capacidade de controlar um processo será afetada – podendo resultar em riscos ambientais, operacionais e até mesmo em perda de vidas. Com sistemas de controle e segurança tornando-se mais convergentes com os sistemas de TI, uma violação cibernética poderia se espalhar mais facilmente para o domínio ICS/OT.

É por isso que uma PHA cibernética adicional é necessária para enfrentar os riscos e ameaças virtuais que caracterizam o cenário industrial dos dias de hoje.

Em um mundo ideal, o primeiro passo seria garantir que o domínio ICS/OT seja resiliente por meio de segmentação da rede. Isso envolve a segmentação da rede em zonas e conduítes e um limite distinto entre os domínios de TI e ICS/OT. Essa é a premissa da IEC 62443, uma série de normas que orientam sobre a segurança desse tipo de domínio. Ela engloba orientação geral, políticas, procedimentos, tecnologia e desenho de sistemas, além dos requisitos de componentes.

De qualquer forma, independentemente de haver ou não segmentação formal de rede, deve existir um foco no fortalecimento da resiliência cibernética, para que as operações possam continuar a funcionar mesmo que um criminoso tenha invadido o perímetro de uma rede.

A PHA cibernética pode ajudar a identificar, verificar e traçar limites no domínio ICS/OT. Ela é uma metodologia voltada para a segurança, que objetiva identificar e avaliar o risco cibernético de domínios ICS/TO e sistemas instrumentados de segurança (SIS). A PHA geralmente segue uma metodologia similar a um HAZOP (*hazard and operability study* — estudo de perigos e operabilidade, em português), mas adaptado especificamente para o ambiente virtual –conhecido como CHAZOP

A PHA cibernética é normalmente realizada em fases, é escalável e pode ser aplicada a sistemas individuais, instalações ou empresas inteiras. São seis as fases principais:

1 Alinhar a equipe do local e o avaliador de ameaças – da equipe de Perigos e Operabilidade (HAZOP) –a respeito da área que deve ser avaliada.

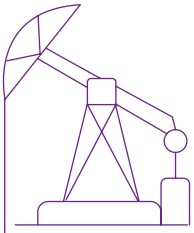
2 Reunir informações sobre os componentes da OT com a rede de OT e o SIS e sobre suas conexões para identificar vulnerabilidades.

3 Analisar as possíveis fragilidades de dados e documentos que poderiam ser exploradas durante um ataque cibernético.

4 Realizar um *workshop* de PHA cibernética para reunir, analisar e integrar informações aos cenários de ameaças, com o propósito de desenvolver um quadro completo dos riscos.

5 Produzir um amplo relatório na conclusão da PHA cibernética, mostrando os riscos dos domínios ICS/OT e SIS e um plano para reduzir os riscos a um nível aceitável para a organização.

6 Preparar um plano de remediação eficaz compreende com uma lista de prioridades de ações, estimativas orçamentárias, programação e necessidades de recursos que, juntos, podem proporcionar níveis de resiliência apropriados.



A PHA cibernética é uma **metodologia voltada para a segurança,** que objetiva identificar e avaliar o risco cibernético de domínios ICS/TO e sistemas instrumentados de segurança (SIS).

O cenário ideal seria realizar a PHA cibernética como uma continuidade da PHA tradicional, baseando-se em suas descobertas para identificar e solucionar qualquer problema virtual.

O resultado da análise deve identificar possíveis perigos e vulnerabilidades e, ao mesmo tempo, fornecer assuntos para discussão dos riscos, gerando recomendações práticas para implementação. Embora o cenário de ameaças à segurança cibernética esteja mudando continuamente, existem classificações gerais dos agentes ou fontes de ameaças que devem ser considerados:

1
Ataque externo técnico

2
Ataque interno não técnico

3
Uso indevido e abuso 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.

Um roteiro detalhado de segurança cibernética pode ser desenvolvido e dividido em: resumo dos principais ganhos, várias remediações de curto prazo e alinhamentos estratégicos de longo prazo para alinhar os programas de segurança de OT e TI.

Benefícios da PHA cibernética

Realizar uma PHA cibernética pode proporcionar vários benefícios. Um deles é assegurar a disponibilidade do sistema ao eliminar o seu risco cibernético. No entanto, esse tipo de avaliação também pode aprimorar outras práticas de negócios de uma organização. A aplicação dessa metodologia documenta os processos e exige a criação de políticas, procedimentos, normas e controles de segurança da informação alinhados com o domínio ICS/OT e com os objetivos da organização.

Principais pontos de melhoria:

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

— Conhecimento de engenharia definido e controles de segurança alinhados, baseados no risco e nos objetivos do negócio.

— Pessoal efetivo confiante devido às funções e responsabilidades estabelecidas.

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

— Resposta cibernética direcionada e priorizada e gerenciamento de incidentes.

— SecOps (Segurança e Operações) com métricas, relatórios e requisitos tecnológicos definidos para ajudar a atingir os objetivos do negócio.

A PHA cibernética também dá visibilidade às organizações do ponto de vista cibernético, a qual pode ser aproveitada para agilizar a convergência entre ICS/OT e TI, ajudando a alcançar o que está se tornando rapidamente um objetivo estratégico vital para muitas empresas.

A convergência entre ICS/OT e TI tem o potencial de criar e simplificar a troca de dados, facilitando as operações de negócios. Contudo, os riscos cibernéticos têm dificultado essa convergência TI/OT. Assim, uma PHA cibernética rigorosa, que ajude a identificar o risco operacional e residual e os ajustes necessários podem fornecer dados que darão confiança à administração para levar adiante a agenda da convergência.

A PHA cibernética no radar regulatório

No entanto, a PHA cibernética não é apenas uma questão de benefícios potenciais para o negócio e para melhores práticas – ela também está no radar regulatório e pode, de várias formas, tornar-se obrigatória nos próximos anos.

De fato, na Arábia Saudita, a Autoridade Cibernética Nacional já lançou uma nova estrutura regulatória para Tecnologia Operacional, que inclui uma revisão especificando que as empresas de petróleo e gás e outras de infraestrutura de circuitos devem realizar uma análise formal dos riscos dos processos que inclua, no mínimo, uma análise qualitativa dos riscos cibernéticos[7].

Se isso for adotado na estrutura, a PHA cibernética estará efetivamente se tornando um requisito regulatório obrigatório e que poderá entrar em vigor ainda este ano.

Enquanto isso, nos EUA, novas medidas foram introduzidas pelo Departamento de Segurança Interna (Department of Homeland Security - DHS) após o ataque cibernético do ano passado a um gasoduto, que interrompeu o fluxo de gasolina, diesel e combustível para o setor de aviação ao longo da costa leste do país. O DHS publicou duas diretivas de segurança da Administração de Segurança do Transporte (Transportation Security Administration - TSA), apresentando diversas medidas para implementação por proprietários e operadores de oleodutos e gasodutos relevantes[8]. A primeira apresenta orientações sobre relatórios de incidentes de segurança cibernética e a nomeação de um coordenador cibernético para organização e avaliação das brechas. Já a segunda é a que realmente tem força, pois exige medidas de mitigação específicas, um plano formal de contingência e resposta e uma revisão anual da arquitetura de segurança cibernética.

Essas exigências, que também incluem a necessidade de realizar uma análise do tráfego de rede nos sistemas de OT, quase podem ser consideradas uma "PHA cibernética leve". O que o DHS está realmente

[7] NATIONAL CYBERSECURITY AUTHORITY. Operational Technology Cybersecurity Controls. 2022.

[8] DEPARTMENT OF HOMELAND SECURITY. DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators. 2021.

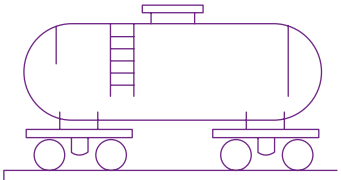
pedindo a essas empresas é que obtenham rapidamente uma avaliação dos componentes e comunicações exclusivos de segurança cibernética do sistema todo e das interdependências de TI e OT e as proteções que estão ou não em vigor.

Em outros lugares, a norma de segurança funcional 61511, da Comissão Eletrotécnica Internacional (International Electrotechnical Commission - IEC) agora exige uma avaliação de risco de segurança do SIS.

O relatório atualizado resume o procedimento de avaliação de risco (PHA cibernética). O *link* para a PHA aqui é um passo na avaliação de risco para, em primeiro lugar, analisar as suas descobertas para identificar as consequências do pior caso de saúde, segurança e meio ambiente (*health, safety, security, and environment* - HSSE) 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 (User Association of Automation Technology in Process Industries - NAMUR), que já publicou a planilha NA 163 — *security assessment of SIS* (avaliação da segurança do SIS).

Aqui, a metodologia de PHA cibernética pode ser utilizada para avaliar os riscos relacionados aos fatores de escalada da segurança cibernética identificados e as mitigações recomendadas para reduzir os riscos a um certo nível. Ao criar uma ponte entre os métodos de PHA e de avaliação de risco de segurança cibernética, os sistemas de segurança se tornam mais robustos contra os ataques à segurança cibernética.



A tendência é que as **exigências regulatórias se tornem mais formalizadas** em torno dos aspectos de segurança operacional relacionados à cibernética – exatamente a área para a qual a PHA cibernética foi desenvolvida.

Em suma, a tendência é que as exigências regulatórias se tornem mais formalizadas em torno dos aspectos de segurança operacional relacionados à cibernética – exatamente a área para a qual a PHA cibernética foi desenvolvida.

Atualmente, podem existir poucos países caminhando em direção à regulação da PHA cibernética, mas esse número pode aumentar bem depressa. Além disso, devido à natureza global e interconectada dos setores de energia e recursos naturais, as exigências em um país provavelmente serão sentidas em outros lugares. Se uma empresa superimportante que opera na Arábia Saudita, por exemplo, for obrigada a realizar uma PHA cibernética, então ela poderá solicitar às organizações aliadas com quem trabalha em outras partes do mundo que façam o mesmo.

Como a KPMG pode ajudar

A KPMG já ajudou clientes liderando e realizando uma PHA cibernética. Nossas equipes multidisciplinares, com ampla experiência no setor, trabalham em estreita colaboração com CISOs, CTOs e equipes de risco no nível corporativo e com gerentes de fábrica, de operações e principais interessados no domínio ICS/OT.

Em um caso, nós ajudamos o cliente de uma empresa que precisava padronizar seus processos em um ambiente de vários fornecedores com sistemas heterogêneos, levando todos ao mesmo nível de segurança operacional. Após uma avaliação das brechas e entrevistas com os interessados, realizamos uma análise baseada na PHA cibernética como parte da resposta com outras avaliações técnicas de segurança, o projeto de zonas e conduítes para dois tipos diferentes de rede ICS e o projeto de painéis de monitoramento para entender melhor a exposição ao risco.

Para discutir qualquer aspecto de uma PHA cibernética e saber como ela se relaciona com sua postura mais ampla de segurança da TI e OT, entre em contato conosco. Afinal, os sinais indicam que exigências da PHA cibernética estão começando a aparecer e podem ser esperadas em breve para um número cada vez maior de empresas industriais.

Fale com o nosso time

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