

OPINIÃO

Cybersegurança na indústria

André Chave

Vice-presidente da unidade de Indústria de Base e Bens de Capital da Falconi

Enquanto a indústria brasileira avança na digitalização de suas operações, as mesmas tecnologias que impulsionam a eficiência abrem portas para ataques cibernéticos. O Brasil concentra 84% de todos os ataques digitais registrados na América Latina, segundo o último relatório Cenário Global de Ameaças da Fortinet. Uma realidade que reforça a urgência de fortalecer a proteção nas plantas industriais.

Entre 2024 e 2025, o setor de manufatura consolidou-se como o principal alvo de ransomware globalmente, conforme o Manufacturing Threat Landscape 2025 da Check Point Software. Uma fábrica parada gera perdas imediatas, o que aumenta significativamente a pressão para pagamento de resgates.

O despreparo corporativo amplifica esse risco. Segundo estudo da Vultus Cybersegurança, 80%

das organizações brasileiras não têm um plano completo para responder a ataques cibernéticos. Simultaneamente, essas ações não apenas crescem em frequência, mas aumentam também em sofisticação, usando inteligência artificial para automatizar invasões e explorar vulnerabilidades em horas, não dias.

Para empresas sem estrutura de resposta, essa janela de tempo é insuficiente. O resultado é uma vulnerabilidade estrutural que coloca a continuidade operacional em risco. A diferença entre um ataque cibernético em um banco e em uma fábrica é medida em vidas. Um incidente de segurança digital em uma planta industrial pode parar linhas de produção, comprometer sistemas de controle, provocar acidentes de trabalho e desorganizar cadeias de suprimento que alimentam centenas de empresas.

Os números são expressivos. Uma paralisação de produção, mesmo que por poucas horas, gera prejuízos milionários e

multas contratuais por atrasos com clientes. Segundo dados da Vultus Cybersegurança, grandes empresas desembolsam em média mais de US\$ 4 milhões por incidente, chegando a US\$ 10 milhões nos casos mais graves.

A vulnerabilidade de um elo fraco na cadeia de suprimentos pode derrubar uma indústria inteira. Um fornecedor invadido não apenas perde seus dados, deixa seus clientes sem matéria-prima, causa atrasos de entrega e desestrutura fluxos de produção que levaram anos para serem otimizados.

Esse “efeito cascata” ultrapassa as fronteiras da TI. A confiança de clientes e parceiros costuma durar menos que o tempo de recuperação de um ataque. Danos reputacionais são, muitas vezes, mais custosos que os financeiros imediatos. Conselhos e diretorias precisam incluir o risco cibernético na pauta de discussões estratégicas, da mesma forma que discutem riscos operacionais e financeiros tradicionais.

Os passos práticos começam ali: definir planos estruturados de resposta a incidentes, estabelecer roteiros de continuidade de negócios, capacitar equipes para reconhecer ameaças e adotar práticas de segurança no dia a dia. Simulações periódicas de invasões, exercícios que testam a resposta da organização sob pressão, detectam fragilidades antes que sejam exploradas por criminosos.

Para a indústria brasileira, a cibersegurança deixou de ser um problema técnico restrito ao departamento de TI e tornou-se questão de continuidade operacional, preservação de empregos e responsabilidade corporativa.

Empresas que constroem defesa robusta contra os ataques não apenas reduzem riscos, ganham velocidade competitiva em um mercado que valoriza resiliência. Investimento em segurança digital é, assim, investimento na própria sobrevivência do negócio e na garantia de quem trabalha nas plantas industriais.



FALCONI/DIVULGAÇÃO/JC



A vulnerabilidade de um elo fraco na cadeia de suprimentos pode derrubar uma indústria inteira.

Quando o risco marítimo chega à bomba de combustível

Larry Carvalho

Advogado especialista em logística, direito marítimo e comércio exterior

Durante décadas, a segurança energética foi analisada sob uma lógica relativamente simples: quanto maior a oferta de petróleo, menor a probabilidade de uma crise. O cenário atual no Oriente Médio demonstra que essa premissa já não explica, sozinha, o funcionamento do mercado global. Hoje, o principal fator de risco deixou de ser apenas a produção. A verdadeira vulnerabilidade está na logística que conecta produtores e consumidores. Petróleo disponível não significa petróleo entregue. Entre um poço e uma refinaria existe uma cadeia formada por navios, seguradoras, armadores, bancos, contratos, rotas marítimas e decisões que passam a ser reavaliadas sempre que a percepção de risco aumenta.

É exatamente isso que acontece com a combinação entre a instabilidade no Estreito de Ormuz e os ataques promovidos pelos Houthis no Mar Vermelho. Pela primeira vez em muitos anos, duas das principais artérias do comércio mundial de energia passaram a sofrer pressão simul-

tânea. O Estreito de Ormuz concentra uma parcela significativa das exportações de petróleo e gás do Golfo Pérsico e não possui alternativas capazes de absorver integralmente esse fluxo. O ponto central, porém, é que ele não precisa ser oficialmente bloqueado para produzir efeitos econômicos. Basta que armadores, seguradoras e operadores logísticos entendam que o risco deixou de ser aceitável.

O mercado marítimo reage muito antes da diplomacia. Diante da incerteza, navios aguardam instruções, alteram rotas ou simplesmente deixam de operar na região. Ao mesmo tempo, seguradoras elevam prêmios, restringem coberturas e incorporam custos que rapidamente se espalham por toda a cadeia global.

Mesmo quando há sinais de distensão política, a normalização operacional leva muito mais tempo. Um cessar-fogo pode ser anunciado em poucas horas. Reconstruir a confiança necessária para deslocar um petroleiro carregado com milhões de barris é um processo infinitamente mais lento. Na tentativa de reduzir a dependência de Ormuz, a Arábia Saudita ampliou o uso de oleo-

duto até sua costa no Mar Vermelho. A solução parecia lógica, até que os Houthis passaram a mirar justamente essa rota alternativa. Quando até os caminhos de contingência se tornam inseguros, o problema deixa de ser regional e passa a afetar toda a arquitetura logística do comércio internacional.

No transporte marítimo, a percepção de risco vale quase tanto quanto o risco efetivamente materializado. Um único ataque pode alterar dezenas de viagens, elevar o seguro em milhões de dólares por operação e tornar financeiramente inviáveis rotas que permanecem abertas do ponto de vista físico.

A conta também não termina no seguro. Rotas mais longas aumentam consumo de combustível, reduzem a disponibilidade de embarcações, pressionam os fretes e elevam custos em diversos segmentos do transporte marítimo. Cada navio que demora semanas adicionais para concluir uma viagem reduz, na prática, a capacidade mundial de movimentação de cargas.

É nesse momento que o Brasil entra na equação. Embora seja um grande produtor de petróleo,

o País continua dependente da importação de derivados, especialmente diesel, e participa de um mercado em que preços são definidos globalmente. Se petróleo, frete, seguro e câmbio sobem simultaneamente, o impacto alcança rapidamente o transporte rodoviário, a indústria, o agro-negócio e, por consequência, o consumidor.

Mais do que uma eventual escassez de combustível, o risco é a formação de uma nova onda de inflação impulsionada pelos custos logísticos. Afinal, praticamente toda atividade econômica depende de transporte.

Existe ainda um componente frequentemente ignorado: as expectativas. Empresas antecipam compras, seguradoras revisam exposições, bancos restringem financiamentos e armadores tornam-se mais seletivos. O custo da incerteza aparece antes mesmo da falta de produtos.

A principal lição dessa crise é que segurança energética e segurança marítima tornaram-se conceitos inseparáveis. Diversificar fornecedores de petróleo já não basta. Será cada vez mais necessário fortalecer rotas, ampliar a capacidade de refino, investir em



LARRY CARVALHO/ARQUIVO PESSOAL/JC

infraestrutura logística e reduzir vulnerabilidades que, até pouco tempo, eram vistas apenas como questões operacionais.

O Brasil está distante de Ormuz e de Bab el-Mandeb no mapa. Mas participa de um mercado em que o preço da energia, do transporte, do seguro e do financiamento é formado globalmente. Em um mundo cada vez mais conectado, a guerra já não altera apenas fronteiras. Ela redefine rotas. E são essas rotas que, no fim da cadeia, ajudam a determinar quanto o consumidor brasileiro pagará na bomba de combustível.