Quadrilhas de hackers promovem ataques cibernéticos e exigem resgates para restabelecer a normalidade dos sistemas de controle da movimentação das cargas

Com uma corrente de comércio de US$ 499,8 bilhões em 2021, sendo US$ 280,4 bilhões em exportações, o Brasil depende da eficiência e agilidade do seu sistema portuário para se manter competitivo no disputado mercado em que está inserido, com predominância de commodities agropecuárias e minerais.

No seu cenário mais realista, o Plano Nacional de Logística 2035, divulgado em 2021, prevê investimentos de R$ 59,5 bilhões no sistema portuário, cujo controle vem sendo progressivamente passado às mãos da iniciativa privada por meio de leilões de concessão.

Para além da necessidade de aparelhamento adequado, uma ameaça global cada vez mais presente vem tirando o sono dos operadores: os ataques cibernéticos feitos por quadrilhas de hackers que exigem resgates vultosos para restabelecer a normalidade dos sistemas informatizados que comandam a movimentação das cargas.

Em 2021, essa máquina oculta de crime digital pode ter alcançado, entre resgates exigidos e prejuízos às atividades, a fantástica cifra de US$ 6 trilhões, segundo estimativa da consultoria alemã Roland Berger, amplamente difundida. O número colocaria a pirataria cibernética, caso ela fosse um país, em terceiro lugar no ranking dos maiores PIBs do mundo, atrás dos Estados Unidos e da China.

Chave-mestre do comércio global, o sistema portuário vem sendo cada vez mais alvo favorito desses ataques. Em julho deste ano, o porto de Los Angeles, um dos mais movimentados do mundo, divulgou publicamente que tem recebido cerca de 40 milhões de tentativas de ataques por mês.

Em fevereiro, ataque a um dos terminais de contêineres do porto de Mombai, o maior da Índia, obrigou o desvio de navios para outros terminais do complexo, provocando atrasos e prejuízos. Em julho do ano passado, outro ataque provocou transtornos por várias semanas nos portos de Durban, Port Elizabeth, Ngqura e Cidade do Cabo, na África do Sul.

No Brasil, o terminal de contêineres do porto de Mucuripe, em Fortaleza (CE), foi alvo de um ataque hacker que causou perturbações no site da Companhia Docas do Ceará (CDC) e provocou lentidão por vários dias, obrigando ao retorno dos sistemas manuais de movimentação de cargas e gerando fila de navios para as operações de carga e descarga.

PROTEÇÃO X CUSTOS

De acordo com o especialista Marcelo Branquinho, fundador e CEO da empresa TI Safe, especializada em sistemas de proteção cibernética, a situação dos portos brasileiros não é das melhores. “Não temos visto uma demanda grande dos portos por proteção. Eles deveriam ter muito cuidado com seus sistemas, mas o fato é que o tema da cibersegurança ainda não despertou fortemente o interesse dos seus dirigentes”, alertou.

Branquinho, que tem atendido grandes empresas do setor elétrico, outro segmento estratégico da infraestrutura, e vem negociando com alguns portos, disse que uma das razões para a baixa demanda portuária e em outros setores é que “as empresas enxergam a cibersegurança como custo, um dinheiro que elas vão gastar e não vão gerar payback”.

Essa avaliação, para o especialista, é superficial e perigosa. “O que está em jogo é a atividade- -fim daquelas empresas. Elas não percebem que aquilo que vão deixar de gastar em cibersegurança podem perder em horas de um ataque de hackers”, disse.

Branquinho explicou que esses ataques se intensificaram desde o começo da pandemia da Covid-19, quando grande parte dos empregados dos escritórios dos portos e das empresas em geral passaram a trabalhar de casa, em regime de home office.

A mudança, segundo ele, não foi acompanhada dos cuidados necessários ao trabalho em ambiente digital. Os funcionários passaram a acessar de casa os sistemas dos portos, facilitando a tarefa dos piratas, especialmente com o uso do chamado ransomware, um tipo de software maldoso que "sequestra" a chave de segurança do sistema de informática do porto e passa a exigir um resgate, a ser pago em moeda digital (bitcoin).

O especialista explica que, mais complexo do que o sequestro físico propriamente dito, o da chave digital pode não se resolver com o pagamento do resgate. Satisfeita a exigência, em geral com a negociação de um valor menor do que o pedido inicial, o hacker continua com a chave da empresa e nada impede que ele venha a fazer um novo ataque e novas exigências.

Como há nos portos equipamentos que não têm segurança em si, Branquinho aconselha que os terminais cerquem esses equipamentos de um modelo de proteção chamado de "zona de conduit", baseado na norma internacional ISA/IEC 62443, específica para segurança cibernética.

Resumidamente, o modelo recomenda separar as redes em zonas de segurança e proteger o entorno dessas zonas, como fazem no mundo físico os bancos com seus cofres de valores. A proteção inclui instalar dispositivos de controle de entrada e saída de informações (firewells) nos casos de redes que se comunicam com terceiros e ITS industrial, que são equipamentos destinados a detectar comportamentos estranhos dentro das redes.

Entre outras soluções recomendadas por Branquinho aos portos estão o anti-malware industrial, que é o antigo antivírus com sistemas inteligentes, sistemas de controle ao acesso remoto, treinamento rigoroso do pessoal quanto às políticas de segurança e instalação de backups que assegurem o retorno rápido das operações.

APÓLICES DE SEGUROS

Outro recurso para proteger os portos e os navios que asseguram o comércio exterior contra os prejuízos dos ataques cibernéticos é a compra de seguro. No caso dos portos e do transporte marítimo, há o seguro cyber, que é geral para todos os setores, e o seguro marítimo, voltado para os danos físicos aos equipamentos. E eles começam a construir pontes entre si.

"Há o ramo marítimo e o ramo cibernético e existe o meio termo, algo que está em uma espécie de limbo, que é o ataque cibernético marítimo", explica Guilherme Mattoso, líder da Área Marítima da corretora Gallagher.

Segundo Mattoso, a busca desse meio termo começou a acontecer a partir de uma série de exclusões colocadas na apólice do seguro marítimo, geralmente imposta pelo segmento de resseguros, que tornava a situação muito difícil para comprovar a responsabilidade do ataque cibernético por um dano físico a um navio, por exemplo.

O especialista da Gallagher exemplifica com o caso de um navio que sofreu ataque de hacker um blecaute- deixando-o à deriva e, na sequência, fazendo-o encalhar com perda do casco.

No caso, o segurador buscava demonstrar que o dano físico decorreu do impacto do encalhe e que o ataque cibernético teve participação, mas não foi determinante, uma vez que haveria alternativas para evitar esse impacto, como o uso de carta náutica física ou até de um tripulante para vigiar a permanência na rota, como nos tempos do cesto de gávea.

"Só que essas exclusões de cyber impostas pelo mercado de resseguros e implantadas meio que obrigatoriamente tornaram-se exclusões muito fortes", explica. A ponto, por exemplo, da exclusão de cobertura para o hipotético caso de um ataque remoto a um equipamento que fizesse este

soltar a carga que estava movimentando e causar um dano a alguém.

Diante do quadro, segundo Mattoso, o seguro marítimo começou a oferecer coberturas complementares como paliativos às exclusões. Paralelamente, o seguro cyber começou a oferecer coberturas mais complexas para a parte de escritórios do cliente e, desse esforço simultâneo, nasceu o meio termo, o seguro cyber marítimo.

No caso das embarcações, o especialista explica que elas estão cada vez mais tecnológicas, principalmente aquelas de apoio à indústria de petróleo offshore, e conectadas à base de apoio no porto de onde podem ser operadas automaticamente como ocorre, por exemplo, com os carros de corrida.

Um ataque a essa base em terra pode gerar ordens contraditórias que resultem em danos às embarcações. Para prevenir esses riscos, o mercado de regulação está passando a emitir cada vez mais regras de segurança cibernética para conceder a certificação dessas embarcações. Um exemplo básico é a segregação entre a intranet e a internet usada pelos tripulantes para falar com suas famílias.

CUSTO ELEVADO

Como consequência de todos esses riscos e do crescimento exponencial do mercado de seguro cyber a partir de 2020 (pandemia), passando de R$ 25 milhões em 2018/2019 para R$ 105 milhões em 2021, Daniela Reia, líder de Placement da Gallagher, explica que o mercado segurador passou a ajudar as empresas a encontrar o melhor caminho para se protegerem.

“O mercado segurador tem um papel fundamental, que é o desenvolvimento da cultura desses cuidados, por exemplo, definindo os sistemas mínimos de proteção para se ter acesso a esse tipo de seguro”, explica. A lista inclui basicamente aquelas proteções sugeridas acima por Branquinho, ressaltando a necessidade de se ter um sistema de gestão de PET para atualização de softwares.

No caso dos portos, o fato de muitas instalações mais antigas operarem com equipamentos com graus de modernidade diversos, considerados por alguns especialistas como problemáticos para a eficiência das redes de proteção, Daniela ressalva que “não é tão ruim assim” e que os riscos dessas defasagens podem ser mitigados se as instalações operarem em redes segregadas e offline.

O ponto mais importante, segundo a executiva da Gallagher, é que os portos e as empresas em geral tenham consciência da necessidade de se proteger e de treinar suas equipes, para que elas saibam exatamente como detectar riscos em suas máquinas e como agir para evitar esses riscos.

Todo cuidado é pouco porque a sinistralidade é muito alta. Segundo Daniela, alcançou 103% em 2020 e 97% em 2021, ou seja, as indenizações estão niveladas com os prêmios, sem contar com as despesas adicionais das seguradoras, como as obrigações de reservas e os custos administrativos.

O resultado dessa equação é o aumento dos prêmios e, na sequência, a perda de atratividade do segmento para parte do mercado. Segundo Daniela, alguns grupos internacionais de grande porte já estão desistindo de fazer seguro cyber no Brasil, em decorrência do tamanho dos riscos.

Para seguir ofertando o produto, a receita é estimular os investimentos em proteção de modo a reduzir esses riscos e aumentar a atratividade. “Os hackers miram os mais vulneráveis, e os mais vulneráveis são aqueles que não investem em proteção”, resume Daniela.

RISCO INTANGÍVEL

O presidente da Comissão de Linhas Financeiras da FenSeg, João Fontes, responsável pela área de cyber, também destaca que a sinistralidade do segmento está muito elevada e que essa é a razão para o aumento das taxas que vem se verificando no mercado.

“A sinistralidade tem sido bastante elevada, o número de ataques tem crescido muito, basta ler o noticiário”, ressalta. “O segmento marítimo usa pouco o seguro cyber de risco financeiro porque esse produto cobre basicamente o risco intangível, aquela linha financeira relacionada à violação de dados”, acrescenta.

Segundo o executivo, o produto se aplica mais a setores como o de instituições financeiras, de tecnologia e de entidades médicas, empresas que têm em poder dados de terceiros protegidos pela Lei Geral de Proteção de Dados (LGPD).

Isso porque o cyber de riscos financeiros não cobre os danos pessoais e materiais. “Eventualmente, são coberturas de cyber que podem ou não ser oferecidas dentro de outros seguros”, ressalvou.

Mas como o cyber financeiro cobre lucros cessantes, Fontes entende que ele poderia cobrir os prejuízos financeiros, por exemplo, do armador cujo navio não pode carregar ou descarregar em decorrência de um ataque ao porto de destino.

Salvatore Lombardi, CEO da agência Albatroz MGA, entende que o seguro cyber pode minimizar, para as empresas contratantes, as perdas provocadas pela interrupção de uma cadeia logística. “Contudo, não estamos vendo a oferta de seguro cyber para operadores logísticos que possa abranger todos os riscos”, ressalva, na linha dos demais entrevistados.

Lombardi destaca ainda que o seguro de transporte abrange os danos físicos às mercadorias, mas não cobre os riscos de demora, atraso ou lucros cessantes. “O mercado segurador tem a missão de ofertar essa cobertura (mais abrangente) o quanto antes possível, seja por meio de um produto de seguro exclusivamente para ataques cibernéticos, seja por meio de um produto combo”, defendeu.

TOLERÂNCIA ZERO

O consultor especializado na área de cargas conteinerizadas Leandro Carelli Barreto, sócio da empresa Solve Shipping Intelligence, disse que, embora não venha observando reflexos nos fretes e nas taxas portuárias dos crescentes riscos cibernéticos, eles representam um agravante a mais para o risco de caos logístico.

Segundo ele, a maioria das grandes empresas de navegação globais já sofreram algum tipo de ataque cibernético e muitos terminais portuários também. “O que acontece é que as empresas não conseguem fazer booking (reserva de espaço), documentação, recebimento, pagamento, liberação de carga... Isso vai agravando o hoje chamado caos logístico”, disse.

Esse caos decorre de fatores que afetaram profundamente o mercado marítimo nos últimos três anos, decorrentes da pandemia da Covid-19 e da crise geopolítica desencadeada pela guerra na Ucrânia. “O aumento dos ataques cibernéticos pode gerar um efeito cascata nas cadeias logísticas mundiais, que estão com tolerância zero a intercorrências”, apontou.

Embora não esteja informado sobre como os portos brasileiros estão se preparando para enfrentar esses riscos, o consultor disse que atualmente a maioria dos terminais brasileiros é controlada por grandes grupos privados internacionais ou nacionais. Em termos de prevenção, ele avalia que esses grupos estejam fazendo aqui o mesmo que tem sido feito lá fora.

Uma enquete feita pela Associação dos Terminais Portuários Privados (ATP) a pedido da Revista de Seguros, com respostas de cinco terminais, mostrou que nenhum deles sofreu ataque cibernético, mas, de acordo com a entidade, todos eles vêm adotando políticas de segurança e controles de cibersegurança, incluindo testes de invasão, protocolos de governança e segurança de TI e gestão de acessos.

Dos terminais consultados pela ATP, dois informaram ter investido R$ 3 milhões em proteção nos últimos cinco anos, e os outros três disseram não ter uma totalização porque os investimentos são fracionados por várias unidades da empresa. Todos os terminais informaram que têm investido em

atualização tecnológica buscando eliminar, principalmente, as vulnerabilidades recentes.

Em relação aos seguros, todos os terminais consultados pela entidade responderam conhecer a existência de apólices de seguro cyber, mas somente um respondeu ter apólice. Segundo a ATP, os terminais consideram que essas apólices ainda são avaliadas como de “alto custo e cobertura limitada”.

O Ministério da Infraestrutura (Minfra) respondeu, por meio de nota, que a Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis, “concentra esforços para ampliar a efetividade das ações de segurança cibernética”.

Ainda de acordo com o Minfra, são repassadas orientações adicionais às Comissões Estaduais de Segurança Pública da área de portos e navegação, recomendando que adotem uma abordagem mais abrangente e detalhada diante dos crescentes riscos de ataques cibernéticos, com foco em pontos como ligações clandestinas, acessos indevidos a informações, uso de softwares não autorizados e ataques com ransomwares, entre outros.

Matéria publicada originalmente na Revista de Seguros Nº 922

Fonte: CNseg, em 18.10.2022