Problema que paralisou aeroportos, bancos e companhias atuantes em outros setores reforça que ataques por vírus de computador são a principal preocupação de líderes empresariais

O temor se justifica, já que eles podem até paralisar as operações das companhias, causando prejuízos financeiros e à imagem e reputação delas

Nesta sexta-feira, 19, setores de diversos países, incluindo o Brasil, tiveram operações paralisadas ou comprometidas por conta de um apagão causada pelo erro de atualização de um software de uma empresa americana de segurança. Rapidamente, pensou-se que fora causada por um ataque cibernético.

O receio procede, já que ataques cibernéticos são a principal preocupação de líderes empresariais de todo o mundo, de acordo com pesquisa realizada pelo Centro para Estudo de Inovação Financeira (CSFI, na sigla em inglês), do Reino Unido, patrocinada pela PwC. Em todo o mundo, no primeiro trimestre de 2024 houve um aumento de 28% no número de ataques, segundo outro estudo, este feito pela Check Point Research. No Brasil, o crescimento foi ainda maior: 38%.

Nesse cenário, o principal meio de mitigar os danos causados por malwares, phishings, spoofings e afins é o seguro de riscos cibernéticos. A Wiz Corporate, unidade de negócios do grupo Wiz Co (B3: WIZC3) dedicada à distribuição de seguros e produtos financeiros ao mercado B2B, que oferece a solução e está preparada para atender clientes de qualquer segmento ou porte, dá dicas a respeito.

“Estima-se que, por dia, são identificados quase 400 mil malwares. Os passos fundamentais para fortalecer a segurança cibernética nas empresas são: fazer avaliação de segurança, desenvolver políticas de segurança, realizar treinamentos, implementar tecnologias e, principalmente, ter uma apólice de seguro cibernético”, afirma Eduardo Bezerra, head de seguros cibernéticos da Wiz Corporate. “A contratação deste tipo de proteção vem aumentando ano a ano. Podemos dizer que isso se deve a implementação da LGPD nas empresas e aos ataques bem sucedidos que geram desgaste e prejuízo, não apenas financeiro, mas também a imagem e reputação das companhias”, explica o executivo.

As garantias das apólices de seguros cibernéticos são divididas em dois tipos de proteções. As coberturas de respostas a incidentes envolvem os prejuízos do próprio segurado e englobam: serviços de perícia forense digital; custos para restauração e recuperação de dados; pagamento de resgate (extorsão); lucros cessantes por interrupção de rede; gastos de notificação e monitoramento; custos de restituição de imagem pessoal e da sociedade; e custos decorrentes de uma investigação administrativa.

Já as coberturas de responsabilidade civil, que envolvem os prejuízos de terceiros, englobam: custos de defesa; multas e penalidades; responsabilidade por dados pessoais ou corporativos de terceiros; e pagamento por danos decorrentes de uma decisão judicial, arbitral ou acordo.

Aumento da procura

A demanda por seguros cibernéticos cresce na medida em que os ataques se tornam cada vez mais frequentes. De acordo com a Munich Re, uma das maiores companhias de resseguro do mundo em termos de prêmio subscrito, foram US$ 4,7 bilhões em prêmios cibernéticos em todo o mundo em 2018. Em 2021, foram US$ 9,2 bilhões, e a projeção para o final de 2025 é de US$ 22,1 bilhões.

Nesse universo, a corretora de seguros precisa ter um time de especialistas em cibersegurança, fazer uma avaliação de risco, apoiar o cliente na implementação dos controles para, somente depois, ir para a última etapa, que é a contratação do seguro. “Sem uma corretora especializada, aumenta muito a probabilidade de o cliente não receber uma cotação ou a seguradora agravar o valor da apólice por não ficar claro o nível de maturidade do risco analisado”, revela Eduardo Bezerra.

A Wiz Corporate segue alguns passos junto aos seus clientes que procuram pelo seguro cibernético. Primeiro, uma reunião para apresentar a metodologia e forma de identificar e avaliar o risco cibernético da companhia; depois, entrevista com as áreas de tecnologia e segurança da informação para entender o nível de maturidade de cibersegurança; faz então a apresentação do relatório com os gaps e/ou as vulnerabilidades de cibersegurança identificadas pelo time técnico; para, por fim, fazer a colocação do risco junto às seguradoras

Mesmo empresas com um budget já reservado para contratar o serviço enfrentam dificuldades. A principal é ter o nível de maturidade de segurança exigido pelas seguradoras. E o valor do seguro cibernético também sofre influência do segmento de mercado, faturamento, sinistralidade das seguradoras e do limite que o cliente deseja contratar - LMG (Limite Máximo de Garantia).

Fonte: InPress Porter Novelli, em 19.07.2024