Por Rafael Romer

A compra de seguro para proteção contra as consequências de ciberataques ainda é uma modalidade relativamente nova de apólice em todo o mundo. De acordo com um estudo realizado pela consultoria e corretora Aon, globalmente, apenas 19% das empresas possuem algum tipo de seguro que visa proteger a companhia contra eventuais prejuízos financeiros e de imagem decorrentes desse tipo de ameaça.

No Brasil, o mercado é menos desenvolvido ainda: o percentual das companhias nacionais que têm algum produto do tipo contratado não chega a 1% - a Aon, aliás, só fez sua primeira emissão de ciberseguro no país no ano passado, para uma empresa norte-americana de grande escala atuando no mercado nacional.

Mas a empresa aposta que essa realidade deve mudar rapidamente conforme ciberameaças se tornam uma preocupação cada vez mais próxima dos tomadores de decisões de organizações, preocupados em se proteger de possíveis perdas de ativos e reputação após se tornarem alvos de ataques.

Na avaliação de especialistas, uma das tendências que podem movimentar esse mercado é a recente onda de ataques do tipo ramsonware, que "sequestram" dados e documentos através de criptografia e só devolvem as informações ao dono mediante o pagamento de um resgate.

"A gente está falando do sequestro de uma rede, mas há os desdobramentos disso", comentou a diretora da unidade de combate a crimes digitais da Microsoft Brasil, Vanessa Fonseca, durante um debate sobre o tema no Aon Financial Lines Day, em São Paulo. "O dano reputacional, de imagem. Quando você contabiliza isso, tendo seguro é possível manejar de uma forma controlada".

Não há um número consolidado sobre a quantidade de ataques de ramsonwares no Brasil, mas, no ano passado, foram mais de 2,4 mil ataques do tipo relatados por empresas só nos Estados Unidos - número que é bem menor do que a real quantidade de ataques, já que estimativas apontam que só 20% dos ataques de ramsonware são reportados por organizações.

Outro fator que pode motivar a adoção desse tipo de dispositivo de proteção no país é a expectativa de uma mudança na legislação brasileira até o final do ano, principalmente no que diz respeito à obrigatoriedade de notificação de ataques recebidos por empresas. Hoje, companhias atuando no Brasil não têm obrigação legal de divulgar informações para clientes ou acionistas sobre possíveis dados de ciberataques sofridos - algo que já é obrigatório por lei em países como os Estados Unidos.

Se aprovada, a legislação passaria a exigir que companhias façam a divulgação de informações sobre o prejuízo financeiro e de perda de dados após sofrerem um ataque, o que deve aumentar a pressão sobre as empresas que quiserem minimizar o impacto reputacional negativo após a divulgação. Nestes casos, o ciberseguro teria o potencial de diminuir dano a imagem da empresa.

"Eu diria que é uma modalidade obrigatória em função dos riscos, que são irreversíveis", comentou Renato Blum, advogado especialista em direito digital. "Vejo até como uma ferramenta de marketing para qualquer empresa. 'Eu tenho esse seguro de proteção de dados que vai me auxiliar em uma situação de vulnerabilidade ou indesejada'".

Fonte: Canaltech, em 16.06.2016.