Ataques cibernéticos recentes acendem alarme para a importância de as empresas investirem em ciberseguros

Invasões a sistemas de empresas dos mais diversos setores e de tribunais deixam cada vez mais evidentes os riscos de prejuízos financeiros e reputacionais que as organizações correm diariamente

Marcelo Barsotti, CCO da Pryor Global

Os ataques cibernéticos têm crescido exponencialmente nos últimos anos, mas este ano foram acrescentadas à lista de invasões nacionais algumas organizações com sólida reputação no mercado, como Americanas, Localiza, Sascar e Sebrai, além de importantes tribunais. Todas

detentoras de grandes mailings de consumidores brasileiros e, por consequência, amplos volumes de dados sensíveis e pessoais.

A tendência é que as ações dos criminosos cibernéticos continuem a crescer e a surpreender em termos de criatividade e astúcia. Isto porque a presença on-line continuará prevalecendo em função da digitalização de grande parte das atividades cotidianas. Dados recentes da Check Point Software, por exemplo, indicaram um aumento global de 40% no número médio de ataques por semana entre 2020 e 2021, sendo que n o Brasil, um dos principais alvos dos hackers, esse aumento chegou a 62% .

Os números para 2022, certamente, serão superiores, o que exige cada vez mais investimentos das empresas em prevenção, em todos os sentidos, inclusive em seguros que garantam a cobertura dos prejuízos financeiros gerados e das eventuais agruras causadas a consumidores que tenham seus dados vazados. “Por mais que as empresas invistam no aperfeiçoamento de suas infraestruturas e em segurança da informação, precisam garantir respaldo financeiro para cobrir eventuais invasões e vazamentos de informações ou mesmo a necessidade de pagamento de resgates para garantir sua continuidade operacional” afirma Marcelo Barsotti, CCO da Pryor Global.

Segundo ele, por esta razão, é natural que a procura e contratação de ciberseguros esteja crescendo e que as apólices estejam cada vez mais assertivas na cobertura de necessidades específicas de cada companhia. “Os casos de ransomware têm se destacado pela engenhosidade das táticas de hacking e extorsão usadas por criminosos, mas existem diferentes tipos de ataques cibernéticos e todas as empresas possuem algum grau de vulnerabilidade. Engana-se quem pensa que apenas grandes corporações e governos são alvos de ataques. As pequenas empresas também registraram incidentes no ano passado e também precisam se proteger com seguros”, alerta Barsotti.

O executivo da Pryor Global ressalta que é preciso escolher um seguro cibernético, cujas coberturas sejam adequadas às necessidades específicas de cada empresa e que ajude a empresa a prevenir-se de eventuais processos gerados por vazamentos ou equívocos nos tratamentos de dados, que podem gerar multas e punições em função da Lei Geral de Proteção de Dados (LGPD).

O seguro cibernético ajuda a cobrir os custos de uma crise causada por crimes cibernéticos, garantindo riscos patrimoniais e responsabilidade civil. A cobertura, dependendo das cláusulas

contratuais, pode garantir o pagamento de resgate de dados em casos de extorsão, despesas para contenção de vazamento de dados, custos de defesa cibernética, condenações civis e multas administrativas aplicadas a terceiros, entre outros prejuízos. “Dada a natureza dinâmica do ambiente digital, é fundamental ainda contar com corretores especializados, que conheçam o assunto e entendam o negócio da companhia, de acordo com seu porte, setor e vulnerabilidades específicas”, diz Barsotti.

Fonte: INK, em 06.04.2022