

Por Sidney Dias (*)

A sigla LGPD (Lei Geral de Proteção de Dados) já se tornou familiar para a maior parte das empresas e organizações. Ela também foi incorporada ao cotidiano das pessoas físicas que tratam dados como parte de seu negócio – como dentistas, médicos, contadores e corretores de seguros, por exemplo.

Em vigor desde setembro de 2020, a LGPD prevê a possibilidade de penas, que podem ser aplicadas pela ANPD (Autoridade Nacional de Proteção de Dados), chegando a R\$ 50 milhões por infração.

As notícias sobre ataques por hackers a empresas e órgãos de governo em todo o mundo têm mostrado a importância de o gerenciamento de riscos endereçar essas ameaças. Veja alguns dos ataques que chamaram a atenção em 2021:

>> Em maio a Colonial Pipeline, operadora do maior sistema de dutos de gasolina e diesel dos Estados Unidos sofreu um ataque que a levou a desligar seus sistemas, comprometendo o fornecimento de produtos de petróleo refinado para postos de gasolina na costa leste do país. Segundo informações divulgadas na mídia, a empresa teria pago resgate de quase US\$ 5 milhões.

>> Também em maio, a brasileira JBS sofreu um ataque que comprometeu suas operações nos Estados Unidos. Segundo informações divulgadas, o retorno à normalidade só ocorreu após o pagamento de resgate de US\$ 11 milhões.

>> Em junho, o Laboratório Fleury foi alvo de tentativa de ataque que afetou, durante uma semana, o sistema de acessos da empresa de diagnósticos.

>> Em outubro, a Porto Seguro, uma das maiores seguradoras do Brasil, sofreu um ataque que causou instabilidade nos canais de atendimento e de alguns sistemas da empresa.

>> Também em outubro, a Atento, uma grande provedora de serviços de call center, sofreu ataques que trouxeram impactos para os serviços de atendimento de vários clientes – dentre eles empresas financeiras, operadoras de planos de saúde e seguradoras.

>> Em novembro/2021, o iFood sofreu um ataque que trocou nomes de restaurantes por mensagens de cunho político. A empresa informou, à época, não ter identificado vazamento de dados pessoais.

>> Em dezembro, o site do Ministério da Saúde foi invadido por hackers, que impediram o acesso aos dados sobre a vacinação contra a pandemia da Covid-19 por vários dias.

Para 2022, os especialistas acreditam que haverá aumento expressivo nos investimentos em medidas de proteção para mitigação dos riscos e na utilização de seguros para redução das perdas financeiras, caso ocorram incidentes que resultem em danos.

A prevenção é a principal medida para reduzir esses riscos. Nessa linha, a tendência é que as seguradoras e seus clientes continuem investindo em duas frentes: na atualização permanente de suas barreiras tecnológicas de defesa e – muito importante – na educação dos seus funcionários para conscientização quanto aos riscos cibernéticos, buscando elevar ainda mais o seu engajamento com a segurança da informação, fortalecendo os seus sistemas de proteção.

(*) **Sidney Dias** é diretor da Conhecer Seguros, mestre e doutor em Informática. Graduado em Administração Pública, é professor em cursos de graduação e pós-graduação e membro de instituições internacionais, como a IEEE/Computer Society, da Association for Computing Machinery (ACM), da Information Systems Audit and Control Association (ISACA) e da International Coach

Federation (ICF). É, também, corretor de seguros habilitado em todos os ramos.

Fonte: Conhecer Seguros, em 11.01.2022