

### **Tais ataques estão entre os cinco riscos mais comuns em curto prazo**

Os ataques cibernéticos estão entre os cinco principais riscos que podem ocorrer em até dois anos, de acordo com o estudo [Global Risk Report 2021](#) feito por uma seguradora, em parceria com as universidades de Oxford e de Singapura e a consultoria de riscos e corretora Marsh & MacLennan. Na edição anterior do estudo, em 2020, eles estavam na 7ª posição em probabilidade e em um horizonte de prazo mais longo.

Os segmentos de serviços médico, financeiro, a indústria de manufatura e o comércio são os mais afetados por ataques cibernéticos e, por consequência, os que mais procuram a modalidade de seguro para esta proteção, embora os ataques podem ocorrer em computadores pessoais.

Hellen Fernandes, especialista em ataques cibernéticos e gerente de Linhas Financeiras da Zurich no Brasil, empresa associada do Sindicato das Seguradoras do Rio de Janeiro e do Espírito Santo, explica como as empresas podem se proteger.

### **SindSeg RJ/ES: Como o seguro cibernético protege as empresas?**

Hellen Fernandes: O seguro é uma de proteção de dados, que ajuda a evitar eventuais perdas financeiras, devido à violação de segurança ou de privacidade de informações. As proteções oferecidas atuam nas seguintes frentes:

- Respostas a incidentes, com coberturas para o pagamento de custos e despesas para ajudar a empresa a lidar com a crise causada por esse vazamento de dados. Neste caso, há a necessidade de contratar especialistas para determinar a extensão do dano, seja em aspectos contábeis, técnicos ou mesmo de imagem. O objetivo aqui é reduzir os efeitos negativos à reputação da empresa.
- Coberturas ao segurado com o pagamento de despesas para recuperar ativos digitais e base de dados, consequentes da interrupção de negócios e de ameaças cibernéticas.
- Cobertura de questões de responsabilidade civil perante as pessoas afetadas (clientes ou funcionários das empresas) ou instituições que os representem por conta do vazamento indevido de seus dados pessoais. Neste caso, o seguro permite o pagamento dos custos de ação civil, coletivas ou individuais, incluindo advogados, para a defesa da instituição e prejuízos financeiros causados às pessoas afetadas, inclusive danos morais.

Porém, além de atuar no pós-incidente, algumas seguradoras também dão o suporte necessário para lidar com a crise, por meio de engenheiros especializados em riscos cibernéticos, para avaliação de riscos, ajudando-as a identificá-los e propondo melhores práticas de gestão do risco.

### **SindSeg RJ/ES: Em que momento a empresa deve contratar um seguro cibernético? Quais são os pontos de atenção nessa contratação?**

HF: Empresas e pessoas são cada vez mais digitais. Consequentemente, tem seus dados cada vez mais expostos no universo on-line, o que explica o crescimento de ataques de hackers - um fenômeno que não é local; é mundial! Soma-se a isso o fato de que muitos usuários passaram a trabalhar em casa por conta da pandemia. Juntos, esses fatores transformaram o que era uma prática esporádica em uma ameaça frequente.

Nesse contexto, as empresas precisam ficar atentas às possíveis vulnerabilidades e, para tal, devem procurar ferramentas para gerir essa questão de maneira adequada e eficiente, buscando conhecimento e proteções de acordo com a legislação e com cada modelo de negócio.

Uma estratégia bem-sucedida de segurança e privacidade de dados passa por criar a consciência

quanto a existência desses riscos dentro da empresa e garantir que haja um engajamento, em especial da alta administração, para garantir que toda essa estratégia seja colocada em prática.

Fonte: FSB, em 06.12.2021