Por Ana Albuquerque

Os escritórios de advocacia são considerados alvos atraentes por criminosos cibernéticos devido ao potencial de acesso a informações confidenciais e que muitas vezes podem envolver grandes somas de dinheiro mantidas sobre processos, negócios e transações de seus clientes. Dados são extremamente valiosos para hackers que podem sequestrar informações e ameaçar empresas em troca de dinheiro, na grande maioria através da modalidade de ataque cibernético, conhecido como ransomware. Importante dizer que o Brasil tem sido um dos principais alvos de ataques de cibernéticos no mundo, tendo o sequestro de dados das empresas o grande objetivo dos cibercriminosos.

Segundo o relatório Allianz Risk Barometer de 2022, os riscos cibernéticos são a principal preocupação para as empresas em todo mundo. Por isso, a segurança cibernética eficaz deve ser uma característica integral de todas as estratégias e dos orçamentos de negócios, independentemente de seu segmento e tamanho.

Em 2020, um ataque ransomware ao STJ (Superior Tribunal de Justiça) impediu o acesso a processos e paralisou os trabalhos do órgão público. Isso prova que a importância ou status não intimidam os criminosos cibernéticos. Anos antes, em outubro de 2017, o escritório de advocacia offshore, Appleby, sofreu uma violação de dados catastrófica que ficou conhecida como Paradise Papers, expondo nomes e informações financeiras de clientes de alto perfil e alto patrimônio.

As medidas necessárias devem ser tomadas pelos escritórios de advocacia para minimizar sua exposição a ataques cibernéticos, especialmente porque esses incidentes estão se tornando cada

vez mais sofisticados. As lideranças devem estar totalmente cientes desse tipo de ameaça aos seus negócios e ter uma compreensão real da exposição potencial.

As consequências de ser vítima de um ataque deste tipo podem ser complicadas e caras, com implicações não apenas para proteção de dados, conformidade regulatória e impacto financeiro, mas também danos à reputação e a preocupação adicional sobre se há cobertura de seguro para tal evento.

Se o escritório não estiver em conformidade com a Lei Geral de Proteção de Dados, (LGPD), por exemplo, as penalidades podem variar entre a aplicação de multas (de até 2% do faturamento, limitado a R$ 50 milhões), suspensão do banco de dados, proibição ou suspensão da atividade de tratamento dos dados e outros.

Apesar das legislações vigentes, a tecnologia continua evoluindo e novas modalidades de crimes aparecem a todo momento. Para pelo menos manter o ritmo, os setores privado e público precisam trabalhar juntos e ter ferramentas eficazes para combater o crime cibernético.

É importante, portanto, que os escritórios de advocacia implementem políticas, controles e procedimentos eficazes e robustos de resposta a incidentes de segurança cibernética, a fim de minimizar sua exposição aos riscos, que devem ser mantidos sob constante revisão e testados regularmente para garantir que sejam eficazes e adequados.

O seguro é uma das ferramentas para proteção financeira em caso deste tipo de ataque, uma vez que cobre, entre outras coisas, prejuízos financeiros devido à reclamação de terceiros por violação de privacidade e segurança da informação; além de perdas do próprio segurado que envolve casos de interrupção de rede e lucros cessantes; restauração dos dados digitais que tenham sido destruídos, perdidos, danificados ou alterados durante um comprometimento de rede, cyber extorsão, entre outros.

A educação contínua e a conscientização também são consideradas ferramentas poderosas disponíveis. É essencial estabelecer uma forte cultura de conscientização cibernética com treinamento regular para todos os membros da equipe, mesmo para o nível mais alto da administração. Embora haja uma maior compreensão desses riscos como resultado do aumento da cobertura de notícias de violações de segurança cibernética e da crescente proeminência na vida das pessoas, esse tema ainda precisa ser trabalhado de forma clara e mostrado como uma questão de extrema importância para a empresa.

Neste momento que avançamos no processo de flexibilização das restrições impostas pela COVID-19 e estamos retomando algumas rotinas presenciais, é uma boa oportunidade para os escritórios reavaliarem suas estratégias de segurança cibernética e revisar suas políticas, controles e procedimentos para avaliar e testar sua eficácia.

Ana Albuquerque
Head de linhas financeiras da WTW Brasil

18.07.2022