Por Daniel Lamboy*

Recentemente, a Securities and Exchange Commission (SEC), agência reguladora do mercado de capitais nos EUA, divulgou a criação de uma regra que tornará obrigatória a comunicação de incidentes cibernéticos por empresas listadas na Bolsa de Valores de Nova Iorque. Isso significa que, quando sofrerem ataques de hackers, essas empresas terão até quatro dias úteis para determinar quais são os “incidentes materiais” e comunicar a ocorrência ao mercado.

A decisão do órgão americano busca dar mais transparência aos investidores das companhias de capital aberto daquele país e possibilitar a compreensão da extensão do risco de segurança cibernética e das políticas e estratégias adotadas pelas empresas na sua mitigação. Incidentes materiais, de acordo com a SEC, são aqueles que os acionistas considerariam relevantes “na tomada de uma decisão de investimento”.

A nova regra deve entrar em vigor no mês de dezembro, ou trinta dias após publicada no Federal Register. O órgão também adotou medidas para obrigar companhias estrangeiras que realizam emissões privadas nos EUA a reportar os ataques cibernéticos ocorridos.

Boa parte das empresas atuando no Brasil são subsidiárias de empresas com exposição no mercado de capitais norte-americana. Seguramente, essas subsidiárias adotarão políticas semelhantes àquelas adotadas nas suas matrizes nos EUA.

A decisão da agência reguladora acontece num momento em que ataques cibernéticos têm se multiplicado. Um exemplo é a exploração de uma vulnerabilidade no MOVEit Transfer, aplicativo de transferência de arquivos gerenciado (MFT) da desenvolvedora Progress Software, largamente utilizado pelas empresas ao redor do mundo.

A Progress Software divulgou uma falha no MOVEit Transfer em 31 de maio e, desde então, mais de 200 companhias disseram ter sido atacadas. O conhecido grupo de ransomware Cl0p assumiu a responsabilidade e publicou dados das empresas alvos em seu site. Segundo o Wall Street Journal, os hackers reivindicaram o ataque de 400 organizações.

Desde o início da crise, 13 processos foram abertos em tribunais federais americanos. Mas os efeitos da exploração de vulnerabilidade como do aplicativo MOVEit Transfer ainda estão longe do fim: quase diariamente há novas companhias afetadas.

O cenário é preocupante, pois o Cl0P é apenas um dos inúmeros grupos de cybercriminosos e as notícias de ataques não param de crescer.

**O contexto da LGPD brasileira para as empresas**

Embora a nova regulamentação americana seja para empresas negociadas em bolsa nos EUA, cabe ressaltar que a LGPD brasileira já previa desde 2020 o dever de comunicar à Autoridade Nacional de Proteção de Dados (ANPD) em caso de incidente cibernético.

O artigo 48 da legislação determina que “o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares”.

Empresas que não respeitarem a lei estarão sujeitas a multas, como aconteceu, por exemplo, com uma companhia brasileira em julho deste ano, na primeira multa aplicada pela ANPD (Autoridade Nacional de Proteção de Dados). A multa, no caso, foi por descumprimento aos artigos 7º e 41 da LGPD, além do Art. 5º do Regulamento Interno da ANPD. Ainda que tais artigos tratem mais da responsabilidade sobre o tratamento dos dados em si e menos sobre o “dever de comunicar”, fato é que a ANPD já está atuando e, autuando, numa sinalização clara ao mercado de que a lei de

proteção de dados brasileira e, sobretudo, as sanções administrativas nela previstas serão aplicadas.

Assim o sendo, seja por necessidade de atendimento de normas impostas às suas matrizes no estrangeiro, seja para o cumprimento da legislação local, empresas instaladas no Brasil precisam estar preparadas. Mas não é suficiente observar a legislação de proteção de dados. Mais do que cumprir o que está na lei, as organizações também devem empenhar esforços cada vez maiores nos mais diversos campos, implementando mecanismos para proteger suas operações, clientes, parceiros e demais stakeholders.

Tais iniciativas visam não somente proteger a empresa de um ataque cibernético, mas também evidenciar, caso ele ocorra, que a organização tomou todas as medidas possíveis para minimizar seu risco. Tais medidas incluem, mas não estão limitadas a iniciativas no campo da tecnologia, conscientização do pessoal, na escolha de parceiros comerciais e, se possível, até na contratação da apólice de seguro compreensivo cibernético.

*__Daniel Lamboy__,
head de Cyber da Marsh Brasil

(12.09.2023)