

Ataques ransomware responderam pela maioria dos acidentes cibernéticos

No momento em que entra em vigor no Brasil a LGPD (Lei Geral de Proteção de Dados), sancionada na última quinta-feira (17) pelo governo brasileiro, o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia, que entrou em vigor em 25 de maio de 2018, completou dois anos.

De lá para cá, alguns fatos marcaram o período. Entre maio de 2018 e novembro de 2019, 22 órgãos reguladores da União Europeia/Área Econômica Europeia (EEE) aplicaram 785 multas às empresas e organizações que violaram dados. Também foram aplicadas multas que chegaram a € 50 milhões (na França) e duas multas que ainda estão em análise no Reino Unido, estimadas em £ 183 e £ 99 milhões.

O dado consta em recente levantamento da consultoria de riscos e corretora de seguros Marsh, produzido a partir de dados do relatório de avaliação bienal da Comissão Europeia (CE) sobre avanços da GDPR. Após entrar em vigor há dois anos, o regulamento vem moldando a regulamentação geral de privacidade de dados em outras jurisdições globais.

O documento ressalta que, mesmo com a continuação do processo de adaptação da GDPR, é provável haver novas interpretações ou mudanças nas leis internacionais de privacidade de dados, especialmente com o aumento da dependência das empresas na tecnologia e as mudanças continuadas no comportamento do consumidor. Por exemplo, acredita-se amplamente que a Covid-19 acelere o uso da tecnologia e dos dados pessoais pelas instituições dos setores público e privado, enquanto os desafios apresentados pela Inteligência Artificial e pelo *machine learning* ainda estão à nossa frente.

Lei de proteção de dados no Brasil

O Brasil foi um dos primeiros países a seguir o exemplo da GDPR da UE ao aprovar a Lei Geral de Proteção de Dados (LGPD), assim criando seu primeiro regulamento de proteção de dados abrangente em agosto de 2018. A lei implantará uma nova Autoridade Nacional de Proteção de Dados, criará direitos fundamentais para as pessoas e exigirá que as empresas comuniquem violações de dados. Como a GDPR, a LGPD tem alcance extraterritorial e se aplica a qualquer empresa que processe os dados pessoais de brasileiros, independentemente da localização da organização.

Impactos nas empresas

O estudo da consultoria aponta que o impacto da GDPR reflete no crescente número de empresas que acionam os seus seguros contra ataques cibernéticos. Os ataques *ransomware* respondem pela maior parte das perdas e paralização dos negócios das empresas.

"Nesse panorama regulatório de rápida evolução, as organizações devem se manter informadas, avaliar continuamente as regulamentações a que estão sujeitas em sua operação e implantar planos de ação de conformidade que incluam uma avaliação do risco da empresa relacionado. Fazer isso para as novas regulamentações pode significar um estímulo mais leve para aquelas organizações que já realizaram este exercício para a GDPR, a LGPD ou outros regulamentos", afirma Marta Schuh, líder de cyber da Marsh Brasil.

"Mesmo as empresas não sujeitas a novas regulamentações em países de atuação deverão avaliar suas práticas de coleta de dados, pois é bem provável que mais nações e estados possam, em breve, aprovar a sua própria legislação", complementa.

Ainda segundo o relatório, neste contexto, as empresas devem revisar os clausulados dos seus seguros para ter melhores chances de recuperação de perdas.

Fonte: Conteúdo, em 25.09.2020