Ransomware e a LGPD

05.10.2021 5 minutos de leitura

Autores

Felipe Palhares

Áreas relacionadas

Proteção de Dados e Cybersecurity

Assuntos

Proteção de Dados e Cybersecurity | LGPD | Felipe Palhares | Segurança Cibernética | Ransomware | Incidentes de segurança

Ataques de ransomware têm se tornado cada vez mais frequentes, sofisticados e agressivos. Não é à toa que alguns países, a exemplo dos Estados Unidos, têm elevado a relevância com que tratam esse tipo de evento, chegando a compará-los a atos que devem ser investigados com o mesmo nível de prioridade de ações terroristas, já que são capazes de provocar uma guerra cibernética. Com a entrada em vigor das sanções administrativas da Lei Geral de Proteção de Dados Pessoais (LGPD), essa prática criminosa começa a ter contornos mais complexos para as organizações que eventualmente sejam atacadas.

Ransomware é uma forma de software malicioso projetado para criptografar os arquivos de um dispositivo ou sistema, de modo que eles não possam ser acessados pela pessoa ou organização que detém respectivos arquivos sem o conhecimento de uma senha criada pelos criminosos. Para revelar a senha que permitirá que os arquivos voltem a ser acessados, os criminosos exigem o pagamento de um resgate, normalmente por meio de criptomoedas, como o Bitcoin. Em outras palavras, o ataque funciona como um sequestro, mas com uma diferença significativa: o alvo do sequestro são os dados guardados pela organização

Os agentes de tratamento não serão responsabilizados quando provarem que o dano é decorrente de culpa de terceiro.

Embora nos primórdios desse tipo de ataque o foco dos atacantes fosse tão somente criptografar as informações, o avanço da adoção de boas práticas de segurança de informação pelas organizações, com o estabelecimento de backups frequentes, que permitem que os sistemas sejam restaurados caso sejam afetados, fez com que as práticas implementadas pelos grupos criminosos também evoluíssem. Além de criptografar os arquivos, os ataques atuais normalmente envolvem a extração de dados da organização, que são utilizados como reféns pelos atacantes. Na falta de pagamento do resgate, os criminosos vazam todas as informações obtidas.

Nesse contexto, a LGPD passa a ser uma faca de dois gumes: ao mesmo tempo em que é fundamental para a estruturação adequada de um sistema nacional de proteção de dados pessoais, também se mostra uma vantagem relevante para os atacantes, que sabem as consequências que um vazamento de dados pessoais pode acarretar para qualquer organização e usam a legislação como pretexto para extorquir recompensas maiores de acordo com a sensibilidade dos dados que foram exfiltrados.

A questão central que merece ser endereçada é até que ponto o custodiante das informações, na figura prevista pela LGPD como o controlador dos dados, é responsável por danos advindos de ataques de ransomware? Em especial, nos casos em que a organização tenha tomado medidas prévias para proteger seu ambiente tecnológico, com a implementação de ferramentas e processos de segurança da informação, é possível punir o controlador por atos criminosos praticados por terceiros?

Os exemplos recentes mostram que nem mesmo o Estado tem sido capaz de se defender de ataques de ransomware, como se pode observar dos incidentes envolvendo o Tesouro Nacional, o Superior Tribunal de Justiça (STJ) e outros órgãos do Poder Judiciário, de modo que parece difícil imaginar que organizações privadas, principalmente de pequeno e médio porte, teriam condições de se defender adequadamente nessa guerra cibernética. Se não se ousa pensar que uma empresa privada seria responsável pelos estragos feitos por um míssil disparado contra um de seus estabelecimentos, haveria margem para responsabilizar a mesma organização pelos danos causados por um míssil digital?

A resposta a esses questionamentos parece estar disposta na própria legislação. De acordo com o inciso III do artigo 43 da LGPD, os agentes de tratamento não serão responsabilizados quando provarem que o dano é decorrente de culpa exclusiva de terceiro, como certamente é um atacante externo ou grupo criminoso. A dificuldade prática para essa exclusão de responsabilidade prevista pela lei talvez seja a aferição da existência de culpa exclusiva

Embora seja verdade que a LGPD impõe um dever de conduta aos agentes de tratamento de implementarem medidas de segurança, técnicas e administrativas, para proteger os dados pessoais tratados, também é fato inconteste que não existe atualmente na legislação, ou em regulamentação da Autoridade Nacional de Proteção de Dados, critérios ou padrões mínimos que precisam ser adotados para esses fins.

Nesse cenário, parece inviável que o regulador, ou mesmo o Poder Judiciário, entendam que os controles implementados por uma organização que foi vítima de um ataque de ransomware eram insuficientes para prevenir o evento, afastando a culpa exclusiva de terceiro por sua ocorrência.

Basta ver que nem mesmo as melhores defesas estão imunes a falhas ou podem garantir que ataques sofisticados sejam efetivamente impedidos, como comprova o ataque bem-sucedido perpetrado este ano contra a FireEye, uma das mais renomadas consultorias de segurança cibernética do mundo. Até mesmo um carro blindado cede a um tiro de bazuca ou a vários tiros disparados exatamente no mesmo lugar. Quando o criminoso ainda possui o suporte de outras nações, como parece ser o caso de diversos grupos que realizam ataques de ransomware, nem mesmo o Iron Dome seria suficiente.

Responsabilizar o agente de tratamento pelo incidente de segurança causado por um ataque de ransomware nessas circunstâncias criaria um precedente perigoso, inclusive para o próprio Estado, que é alvo constante desse tipo de ato criminoso. Afinal, se não há defesa perfeita, nem como garantir proteção total contra eventuais ataques, culpar o motorista do carro em razão da blindagem não ter sido capaz de deter o tiro de bazuca pode ser temerário.

Este artigo foi escrito por nosso sócio Felipe Palhares, da área de Proteção de Dados e Cybersecurity. A publicação foi veiculada pelo Valor Econômico em 04/10/2021, clique aqui e confira o artigo na íntegra.

› PROFISSIONAIS

Profissionais que aliam visão jurídica e visão de mercado

Felipe Palhares