

Em resposta, Renner informa que não há indícios de transferência não autorizada de dados

Logo após o ataque cibernético que a Lojas Renner sofreu em 19 de agosto, o Procon-SP notificou a empresa pedindo explicações sobre o episódio – a empresa foi questionada sobre os bancos de dados atingidos, nível da exposição, período que o site ficou indisponível, se houve vazamento de dados pessoais de clientes e de outras informações estratégicas, plano de proteção e recuperação executado, canais de atendimento disponibilizados aos consumidores durante a ocorrência, entre outras informações.

A Renner respondeu às perguntas e informou que, até o momento, não há indícios de transferência não autorizada de dados, tampouco de que o incidente tenha comprometido a base de dados pessoais gerando risco ou dano relevante aos titulares de dados pessoais. O caso será encaminhado para análise e acompanhamento da equipe de fiscalização.

“As empresas que agirem como controladoras de dados pessoais devem se acautelar no sentido de providenciarem mecanismos de minimização de danos. Mais do que isso, a implementação de compliance digital e estabelecimento de chaves de segurança podem trazer maior confiança quanto ao sigilo de dados dos consumidores”, afirma o diretor executivo do Procon-SP, Fernando Capez.

Esclarecimentos da empresa

A Renner relatou que foi vítima de ataque do tipo ransomware, o qual paralisou parte do seu parque de tecnologia da informação e gerou indisponibilidade temporária do site e aplicativo; que assim que teve ciência do fato alertou os responsáveis; e que o e-commerce foi retomado no site no dia 21/8 e no dia 22/8, no aplicativo.

Sobre a segurança cibernética, esclareceu que adota estratégia em multicamadas e discriminou os controles e ferramentas implementados. Sobre o cadastro no portal informou que ao usuário são solicitados os seguintes dados: e-mail, CPF, nome completo, data de nascimento, telefone e gênero (sendo este último não obrigatório) e que há necessidade de criar login e senha; informou ainda que os dados dos clientes são coletados utilizando criptografia de padrão internacional, sendo possível solicitar a atualização ou exclusão.

Fonte: Procon-SP, em 01.10.2021