A proteção de dados vista como “despesa”
Hacker que expôs falha em empresa aponta falta de “visão” do mercado

por Observatório da Privacidade e Vigilância

O engenheiro de software, Guilherme Berger, conseguiu entrar na página da empresa ingresso.com e comprovar a existência de graves falhas de segurança: além da vulnerabilidade em relação ao extravio de ingressos, detectou facilidades ao acesso de dados pessoais como nome, CPF, RG expostos na web. A falha, exposta em janeiro e abril deste ano, permitia que qualquer pessoa tivesse acesso à lista de ingressos de outros usuários ao acessar uma página da web.
Guilherme desenvolveu um programa simples demonstrando a possibilidade de substituir o código de um ID usuário para outro no endereço de uma página de impressão de ingresso. Deste modo, caso o ingresso interessasse a quem está furtando, bastava imprimi-lo e levá-lo ao teatro, cinema ou show, por exemplo.
Como demonstra em seu blog, foi possível alterar os dados pessoais na face do ingresso para os seus próprios, esquivando-se de qualquer suspeita. Se o burlador chegar antes do cliente real, por exemplo, o código de barras seria validado e ele teria acesso ao evento, enquanto o cliente de fato poderia ficar de fora. Vale lembrar que em 2014, outro artigo foi publicado detalhando duas falhas de segurança semelhantes no site.
De acordo com o hacker, a falha pode ter ocorrido por falta de conhecimento, descaso com a segurança, falta de atenção, ou mesmo “preguiça do desenvolvedor”, porque a “página que listava os ingressos não garantia a segurança dos dados por meio de autenticação e autorização do usuário”, explica.
O engenheiro de software descreve que diversas empresas adotam o modelo de "bug bounty" (recompensas por erro, em tradução livre), onde um pesquisador que descubra uma falha de segurança pode reportar a brecha à empresa e, em troca, ganhar uma recompensa financeira. “Assim o bug (erro) seria corrigido, a empresa ficaria segura, e os pesquisadores seriam motivados a pesquisar e relatar esses erros à empresa”, completa.
Por considerar o que ocorreu na ingresso.com não ser um fato isolado, Guilherme acredita que o mercado em geral, além das agências governamentais, ainda enxergam a proteção de dados pessoais como “custo” e não como investimento que pode gerar “lucro”. “Segurança da informação geralmente é visto não como um "profit center" (centro de lucro, em tradução livre), mas como um "cost center" (centro de custos)”, analisa.
Do ponto de vista do consumidor o caso de má prestação de serviços por parte do Ingresso.com demonstra a urgência de edição da Lei de Proteção de Dados Pessoais, que estabelecerá parâmetros de segurança para os fornecedores de bens e serviços, bem como penalidades para quem descumpra essas obrigações. Isso é o que defende a advogada e conselheira da Associação Brasileira de Defesa do Consumidor (Proteste), Flávia Lefébre.
Para ela, o fato de a empresa apresentar problemas desde 2014 sem solução revela também a necessidade de que se crie um organismo para fiscalizar, apurar infrações quanto às obrigações de guarda segura de dados e de segurança dos sistemas operacionais, bem como para aplicar sanções aos fornecedores que atuem causando prejuízos aos consumidores.
“De qualquer forma, ainda que não tenhamos a lei de proteção de dados pessoais aprovada, o certo é que o Código de Defesa do Consumidor e o Marco Civil da Internet já trazem instrumentos para que se possa afirmar que a omissão da empresa em utilizar mecanismos de segurança eficientes configura vício na prestação do serviço e que, portanto, o usuário da Ingresso.com tem legitimidade para pedir reparação pelos danos sofridos”, lembra a advogada.
Flávia lembra que o art. 20, do Código de Defesa do Consumidor estabelece que: são impróprios os serviços que se mostrem inadequados para os fins que razoavelmente deles se esperam, bem como aqueles que não atendam as normas regulamentares de prestabilidade.
Quanto ao Marco Civil da Internet, ela destaca que o art. 7º postula a garantia da proteção de dados do usuário e, mais, define "a exclusão definitiva dos dados pessoais que tiver fornecido a

determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei".

“Ou seja, é evidente que o mínimo que se pode razoavelmente esperar da ingresso.com é que adote práticas comerciais seguras, já que utiliza dados de cartão de crédito e conta bancária dos consumidores para operar seu serviço e que, depois de concluída a relação de compra de ingressos, os dados sejam excluídos para evitar problemas”, explica.

No início deste ano, um funcionário da empresa informou ao engenheiro de software, Guilherme Berger, que se sabia da falha havia meses, mas que estavam com problemas internos no processo de correção. Após nova repercussão do caso, em abril, um desenvolvedor da empresa comunicou-lhe, via correio eletrônico, que a falha de segurança havia sido corrigida.

O Observatório da Privacidade e Vigilância entrou em contato com a assessoria de imprensa da empresa. Questionada sobre o que tem sido feito para evitar futuras falhas e qual deve ser o procedimento caso os consumidores venham a se sentir prejudicados, expressou-nos que “a segurança sobre as informações dos usuários é prioridade da ingresso.com” e reforçou que “assim que identificou a falha no sistema do aplicativo, a empresa implementou as devidas correções, solucionando a questão”.