Por Alexandre Tamura, Aline Noleto e Tainã Dias (*)

Imagine a seguinte situação: um cliente insatisfeito entra em contato com o suporte de uma instituição financeira, reclamando que não consegue acessar sua conta bancária on-line, pagar um boleto ou sair de uma aplicação financeira que está dando prejuízo. Isso já seria um grande desafio para a instituição, não é mesmo? Agora, pense que essa situação pode ser ainda pior: os dados pessoais desse cliente estão sendo negociados na dark web. Infelizmente, essa não é uma hipótese distante, mas uma realidade cada vez mais comum no mundo cibernético.

Um estudo da Fortinet demonstrou que o volume de tentativas de ataques cibernéticos no Brasil aumentou 16% desde 2021 em comparação a 2022, resultando em incidentes que afetam também a privacidade de titulares de dados. Diante deste cenário, destaca-se a importância das instituições financeiras em manterem a continuidade dos negócios nos níveis previstos pela Resolução BACEN 4577/2017, que dispõe sobre as estruturas de gerenciamento de riscos e de capital, bem como em atenderem aos requisitos estabelecidos pela ANPD (Autoridade Nacional de Proteção de Dados) para gestão de incidentes relacionados à proteção de dados pessoais.

Para seu funcionamento regular, as instituições financeiras coletam e tratam dados cadastrais, de renda, de patrimônio e de conhecimento e apetite ao risco de seus clientes. Essas informações são valiosas para qualquer atacante e, se vazadas, poderão trazer prejuízos financeiros, sanções pelos reguladores e certamente um prejuízo reputacional. Diante do valor de tantos dados, as instituições financeiras também atraem ataques cibernéticos, como o *ramsonware*.

Sabe-se, ainda, que as instituições financeiras investem bastante na proteção dos dados de seus clientes. Mas, e quanto aos prestadores de serviço, como estão em relação à proteção dos dados de correntistas e de investidores? A ANPD já alertou sobre a necessidade de as empresas controladoras de dados de titulares avaliarem e monitorarem a integridade dos serviços prestados pelos seus fornecedores, o que inclui aspectos também relacionados à segurança das informações.

Um ponto relevante a ser monitorado é o acesso de terceiros voltados à implantação e à manutenção de sistemas, que, em termos gerais, não deveria ter acesso à dados reais das instituições e de seus clientes e investidores. Além disso, é crucial que as instituições realizem verificações periódicas em seus fornecedores e sejam rigorosas durante o processo de seleção e

escolha desses prestadores de serviço, visto que incidentes podem ocorrer em terceiros e atingir dados pessoais de clientes das instituições financeiras.

A realização de auditoria em fornecedores somente será possível se houver previsão contratual para tanto, portanto, é relevante que as instituições financeiras revejam tal possibilidade. Ademais, a verificação de controles efetivos e em funcionamento nos prestadores de serviço é de extrema importância, sempre a depender do tipo de serviço e do porte da empresa contratada, ou seja, é necessário garantir que os controles adotados pelo fornecedor sejam adequados ao tipo de informação a ser protegida. Isso inclui:

1. Verificação da estrutura de segurança das informações e de proteção de dados, que permita detecção de eventos de segurança de forma preventiva;
2. Acesso somente às informações necessárias para a execução do serviço contrato, lembrando-se sempre de que dados reais não devem ser utilizados em demais ambientes que não o de produção;
3. Contingência para a continuidade dos serviços contratados, inclusive para situações de indisponibilidade da infraestrutura de TI;
4. Segurança das APIs (Application Programming Interface) que fazem conexão com aplicações da empresa.

É importante lembrar que muitas dessas verificações podem já fazer parte do ISAE – SOC Report, que é um relatório de auditoria independente que atesta a eficácia dos controles internos de uma organização de serviços e pode já ter sido realizado pelo fornecedor, comprovando o bom funcionamento desses controles internos.

Sabemos que as avaliações podem ser feitas de diversas formas e em diferentes momentos, mas é importante destacar que esse processo é contínuo, devendo ocorrer o monitoramento recorrente para verificar se as medidas de segurança estabelecidas estão sendo respeitadas e, assim, em caso de descumprimento, avaliar as ações adequadas para a mitigação de riscos.

Por fim, ressalta-se que as medidas preventivas podem evitar prejuízos às instituições financeiras e, por isso, é de extrema importância utilizar de ferramentas como a avaliação de fornecedores para mitigação de incidentes de segurança da informação envolvendo dados pessoais.

(*) **Alexandre Tamura**, **Aline Noleto** e **Tainã Dias** atuam na área de Data Privacy da Protiviti, empresa especializada em soluções para gestão de riscos, compliance, ESG, auditoria interna, investigação e proteção e privacidade de dados.

Fonte: IMAGE, em 23.06.2023