Wealthsimple confirma violação de dados após ataque à cadeia de suprim

Data: 2025-09-08 16:15:00

Autor: Inteligência Against Invaders

A fintech canadense Wealthsimple confirmou uma violação de dados que expôs informações confidenciais pertencentes a cerca de 30.000 clientes. O incidente, detectado em 30 de agosto, foi atribuído a um software comprometido fornecido por um fornecedor terceirizado.

De acordo com Riquezasimples, os dados expostos incluíam detalhes de contato, identidades emitidas pelo governo, números de seguro social, datas de nascimento, endereços IP e números de contas. A empresa enfatizou que as senhas não foram comprometidas, nenhuma conta de cliente foi acessada e nenhum fundo foi roubado.

A empresa também disse que agiu rapidamente, contendo a intrusão em poucas horas. Sua equipe de segurança interna, apoiada por especialistas externos, iniciou uma investigação e notificou os reguladores financeiros e de privacidade. Todos os clientes afetados receberam comunicação direta por e-mail até 5 de setembro.

Suporte para clientes afetados

A Wealthsimple introduziu um pacote de medidas de apoio, incluindo:

- Dois anos de acompanhamento gratuito de crédito
- Monitoramento da dark web
- Proteção contra roubo de identidade e seguro
- Uma equipe de suporte dedicada para clientes afetados

Leia mais sobre violações de dados no Canadá: Regulador financeiro canadense hackeado,

expondo dados pessoais de organizações membros

Riscos cibernéticos em ascensão

A violação da Wealthsimple faz parte de uma tendência mais ampla de incidentes cibernéticos no Canadá.

Nos últimos meses, a Câmara dos Comuns, WestJet e vários conselhos escolares de Ontário relataram ataques.

Um estudo da IBM divulgado neste verão descobriu que o custo médio de uma violação de dados no Canadá subiu para US$ 6,98 milhões, com violações no setor financeiro em média de quase US$ 10 milhões.

A Wealthsimple, que administra mais de C$ 84 bilhões (US$ 60 milhões) em ativos de clientes, disse que desde então aprimorou suas defesas para evitar incidentes semelhantes. A empresa pediu aos clientes que habilitem a autenticação de dois fatores, usem senhas fortes e exclusivas e fiquem atentos a tentativas de phishing.

“Obrigado, como sempre, pela confiança que depositaram em nós. Levamos isso muito a sério”, concluiu a empresa.