

Grande varejista brasileira automatiza proteção de mais de 50 milhões de clientes com a Axur

🎯 Problema

Invasores podiam usar cadastros comprometidos sem o consentimento das vítimas para acessar dados, testar cartões roubados ou realizar atividades que comprometem a experiência do usuário. Usar uma conta comprometida é mais fácil do que criar uma nova usando dados roubados. O trabalho manual dos analistas tinha se tornado mecânico e dispendioso, especialmente em períodos críticos como a Black Friday, quando a celeridade é imprescindível.

Sobre a empresa

Uma das maiores varejistas on-line do Brasil, com mais de 50 milhões de clientes cadastrados. A empresa opera em escala nacional e enfrenta desafios típicos do e-commerce de alto volume, especialmente em datas críticas como a Black Friday.

💡 Solução

A equipe de segurança implementou uma automação que consulta a base de vazamentos por meio da API da Axur, aproveitando filtros configurados na plataforma que entregam apenas as credenciais relevantes.

O script serve de ponte entre a Plataforma Axur e os sistemas internos, realizando reset de senhas de forma transparente para o usuário.

Impacto na operação



Mais de 1,5 mil contas tratadas automaticamente desde a implementação



Eliminação total da fila de tratamento manual




100% das credenciais vazadas resetadas automaticamente



Black Friday 2022 como marco de implementação bem-sucedida

"Graças ao pessoal de desenvolvimento da Axur, temos o consumo dos dados via API que nos permite automatizar esse processo todo. Hoje basicamente toda credencial vazada foi resetada e temos a segurança que não será usada de forma fraudulenta."

 **Analista de Segurança**
Grande Varejista Brasileira





O desafio da escala em períodos críticos

Antes da automação, os analistas realizavam manualmente a transposição dos dados da Plataforma Axur para os sistemas internos. Com a proximidade da Black Friday 2022, ficou evidente que esse modelo não seria escalável para atender à alta demanda de um dos períodos mais críticos do e-commerce brasileiro.

Embora o comprometimento de credenciais ocorra fora do perímetro da empresa, seus impactos recaem diretamente sobre o varejista, afetando a experiência do usuário e gerando custos adicionais com suporte, recuperação de contas e prevenção a fraudes.



Proteção transparente e proativa

A resposta ao incidente é transparente para o usuário, que só é solicitado a trocar a senha ao realizar ações sensíveis, como a finalização de uma compra. Esse modelo reduz o atrito e preserva a experiência do cliente durante a navegação.

Ao acelerar o tratamento dos incidentes, a automação diminuiu significativamente a janela de exploração das credenciais vazadas, permitindo que sejam invalidadas antes que possam ser utilizadas em atividades maliciosas.



Automação que evolui continuamente

As primeiras versões da automação ainda exigiam intervenção dos analistas para adaptar os dados recebidos. A cada nova etapa, o processo ganhou eficiência e reduziu o esforço operacional, acompanhando o aumento do volume de incidentes.

Com a adoção de filtros e da API da Axur, o fluxo passou a receber apenas credenciais relevantes e evoluiu até se tornar totalmente automatizado, consumindo, preparando e processando os dados de ponta a ponta, sem necessidade de ação humana.



Integração que potencializa resultados

A varejista já possuía processos internos e APIs maduras, capazes de sustentar uma automação desse porte. A equipe de segurança identificou que bastava criar um script para conectar a Plataforma Axur aos sistemas internos existentes.

Com o monitoramento de ambientes externos, incluindo Deep & Dark Web, a Plataforma Axur entrega alertas filtrados e relevantes, garantindo visibilidade antecipada sobre vazamentos e permitindo uma resposta rápida, precisa e escalável.

Descubra como automatizar a proteção dos seus clientes

AGENDE UMA DEMO

Gartner
Peer Insights.  4.9
★★★★★

Conheça todas as nossas soluções: axur.com

///AXUR