

Líder do setor de moda da Fortune 500 protegeu APIs e operações de varejo

APIs que abastecem experiências de varejo convenientes e personalizadas foram protegidas e os dados dos clientes foram protegidos contra violações



Descobriu todas as APIs



Identificou vulnerabilidades



Melhorou a postura de segurança

As APIs têm desempenhado um papel integral na transformação do setor de varejo de lojas físicas tradicionais para plataformas de comércio eletrônico. Há uma API por trás de cada interação digital, o que permite que varejistas:

- Conectem vários sistemas, aplicativos e serviços com facilidade
- Integrem suas lojas online com sistemas de gerenciamento de inventário de back-end, gateways de pagamento, provedores de envio e ferramentas de gestão de relacionamento com o cliente
- Facilitem uma rápida troca de dados que deixa o varejo online personalizado e conveniente

Com a proteção desses dados como prioridade máxima, a segurança de APIs desempenha um papel fundamental na garantia da confiança, integridade e confidencialidade das operações de negócios online.

A proximidade constante das APIs com dados confidenciais as torna alvos atraentes para **cibercriminosos** que buscam explorar vulnerabilidades. Uma violação de APIs bem-sucedida pode levar à exposição de informações do cliente, como dados pessoais, dados do cartão de pagamento e histórico de compras. Por essa razão, este varejista de moda da Fortune 500 recorreu à Nomenclatura Security (agora uma empresa Akamai) para receber ajuda, já que a empresa já estava insatisfeita com sua relação com a Salt Security.



Localização

Estados Unidos

Setor

Varejo

Solução

Akamai API Security

Criação de uma abordagem programática para a segurança de APIs

O varejista da Fortune 500 queria criar um fluxo de trabalho completo de ponta a ponta para mitigar os riscos de segurança de APIs para além dos [firewalls de aplicativos da Web](#) e [gateways de APIs](#). Isso exigiria uma estratégia sólida de segurança de APIs, com controles robustos para a governança de APIs. A empresa também estava focada na mitigação de bots, para essencialmente distinguir entre usuários legítimos e bots mal-intencionados, permitindo proteger seus sistemas, dados e experiência do usuário.

Dado o tamanho do projeto, o varejista e a Akamai concordaram em uma abordagem em fases. A primeira fase implicaria localizar todas as APIs, classificar dados confidenciais, implementar detecção e resposta, bem como fazer a integração com o Splunk. A segunda fase implicaria o uso de uma abordagem de teste de segurança de APIs do tipo "shift-left" para acelerar a criação de código seguro.

A implantação acelerada diminuiu o tempo de valorização

Apesar da primeira fase ser complexa, a equipe Akamai conseguiu implantar os módulos de descoberta de APIs e proteção de tempo de execução da Noname, enquanto executava a integração do Splunk, em apenas 120 dias. A descoberta de APIs desempenha um papel fundamental na gestão da multiplicação de APIs. Ela envolve a identificação sistemática e catalogação de todas as APIs dentro de uma organização. Ao manter um repositório centralizado de APIs, os desenvolvedores podem facilmente pesquisar e descobrir APIs existentes antes de embarcar em novos esforços de desenvolvimento. Isso ajuda a eliminar a duplicação e promove a reutilização, economizando tempo e esforço.

A Akamai usa a detecção automatizada baseada em aprendizado de máquina para identificar vulnerabilidades de APIs, incluindo vazamento de dados, adulteração de dados, violações de políticas de dados, comportamento suspeito e ataques à segurança de APIs. O varejista da Fortune 500 pode melhorar significativamente a segurança e a integridade de suas APIs, proteger dados confidenciais e manter a confiança de usuários e parceiros.

