História do cliente da Akamai

Varejista de bebidas da Fortune 100 protege APIs e dados

Os dados do cliente são protegidos pela identificação das principais vulnerabilidades de APIs e pela reparação dos danos causados por fraude, abuso e roubo anteriores

Interfaces de programação de aplicativos, ou APIs, permitem que os varejistas criem experiências personalizadas completas para os clientes, ao mesmo tempo em que simplificam as operações. Todas as variáveis que colocam uma bebida nas mãos dos consumidores, incluindo dados de estoque, envios de pedidos, dados de localização, pagamentos e até programas de recompensas, são entregues pelas APIs. As APIs revolucionaram a experiência de compra conectando o ecossistema de varejistas, seus parceiros e seus clientes. Mas sua proximidade constante com dados confidenciais também as torna um risco.

Embora os consumidores desfrutem da nova experiência de varejo digital, eles estão frequentemente preocupados com o quão bem suas informações pessoais são protegidas, e com razão. As APIs estão se tornando cada vez mais um vetor de ataque preferido pelos cibercriminosos. Por esse motivo, uma empresa de bebidas de varejo da Fortune 100 procurou a Noname Security (agora uma empresa Akamai) para lidar com vulnerabilidades em sua postura de segurança de APIs.

Desafios de uma crescente pegada de APIs

Em nossas conversas iniciais, a empresa expressou preocupações sobre sua incapacidade de alcançar governança e segurança de APIs significativas em escala global. Para reunir evidências, encomendou uma recompensa por bugs documentados publicamente que identificou uma enorme vulnerabilidade. Os nomes, endereços, e-mails e números de telefone de quase 100 milhões de usuários poderiam ter sido exfiltrados. Felizmente, esse era um programa de recompensas, e os problemas foram corrigidos sem danos.

Retail Beverage Company

Localização

Estados Unidos

Setor

Varejo, viagens e hotelaria

Solução

Akamai API Security

Principais impactos

- Bilhões de chamadas de APIs protegidas por dia
- 5.000 solicitações seguras por segundo
- Mais de 200 problemas identificados e resolvidos

Akamai

A empresa também teve visibilidade e monitoramento inadequados de APIs de produção, o que resultou em uma incapacidade de avaliar adequadamente os riscos, e seus dados Apigee não forneceram detalhes contextuais (por exemplo, tipos de dados, comportamento do usuário, linhas de base, análise forense de vulnerabilidade). Devido a essas vulnerabilidades de APIs, ocorreram fraude, abuso e roubo. Isso levou a altos custos operacionais para o varejista.

Fortalecimento da sua postura de segurança de APIs

A plataforma de segurança de APIs da Noname (agora parte do Akamai API Security) conseguiu inventariar as APIs do cliente e fornecer análises comportamentais, detecção de ataques em tempo real e gerenciamento de vulnerabilidades, incluindo testes AppDev específicos de API. Como resultado, o cliente foi capaz de detectar e corrigir ataques a APIs que não foram detectados pelos controles existentes. A equipe de segurança de aplicativos, ou AppSec, conseguiu aumentar a eficiência e melhorar a priorização de problemas de alto risco.

A Akamai também suporta até 50.000 APIs por mecanismo sem latência operacional. Com nossa plataforma como o núcleo, o cliente desenvolveu um programa global de segurança de APIs. Agora, desfruta de total visibilidade em seu inventário de APIs com detalhes de API contextualmente relevantes. Além disso, a empresa ganhou inteligência acionável que não estava disponível com as ferramentas existentes. Isso permitiu recursos econômicos para gerenciamento eficiente de vulnerabilidades de APIs e detecção de ameaças em tempo real.

 | Publicado em 08/24