História do cliente da Akamai

Empresa financeira descobre e protege APIs

Um banco protegeu suas iniciativas digitais com a descoberta de APIs ocultas, avaliando e mitigando o risco às APIs e atendendo às demandas regulatórias

Ganhou visibilidade completa

Aprimorou a postura de segurança

Protegeu iniciativas digitais

O setor de serviços financeiros está rapidamente adotando a transformação digital para se manter competitivo em um mercado em constante evolução. Ao usar recursos digitais, como inteligência artificial e análise de big data, as instituições financeiras podem oferecer produtos inovadores, reduzir custos e fornecer serviços mais personalizados e eficientes aos clientes.

Ao mesmo tempo, a transformação digital traz consigo um maior risco de ataques cibernéticos. Para combater esse problema crescente, a cibersegurança é agora parte essencial de qualquer estratégia de transformação digital. As empresas de serviços financeiros devem garantir que seus sistemas sejam seguros e resilientes para proteger os dados e ativos dos clientes contra agentes mal-intencionados.

Um dos principais bancos comerciais da Ásia rapidamente procurou a Noname Security (agora uma empresa Akamai) para ajudar a fortalecer sua postura de segurança de APIs. As violações de API atingiram taxas alarmantes; a Tech Wire Ásia apontou que "hoje, 1 em cada 13 incidentes cibernéticos podem ser atribuídos à insegurança das APIs". Eles também enfatizam que "as vulnerabilidades de APIs custam às empresas até US$ 75 bilhões anualmente".

Considerando que nosso cliente tem mais de US$ 700 bilhões em total de ativos, mais de 5.000 clientes corporativos e uma reputação de gerenciamento patrimonial mundialmente renomada, era imperativo que todas as vulnerabilidades de APIs fossem abordadas o mais rápido possível.

Financial Services

Localização

Ásia

Setor

Serviços financeiros

Solução

Akamai API Security

Akamai

Necessidade de maior visibilidade das APIs e seus riscos

A instituição já havia implantado uma plataforma de gerenciamento de APIs para autenticação e controle de tráfego, mas havia dúvidas sobre sua capacidade de prevenir o abuso de APIs e ataques cibernéticos. Embora os gateways de APIs forneçam controles básicos de segurança de APIs, que são muito necessários, eles infelizmente não são suficientes para proteger adequadamente as organizações contra ameaças específicas às APIs.

Por exemplo, a autorização em nível de objeto corrompida, muitas vezes referida como BOLA, aparece como tráfego normal de APIs para gateways. Essa falta de conscientização contextual entre solicitações e respostas de APIs permite que os ataques de BOLA passem sem serem detectados e acessem serviços de back-end importantes. Essa falha não só pode deixar as organizações vulneráveis às explorações do BOLA, como também pode abrir a porta para outros ataques e abusos de lógica empresarial.

Outra limitação de visibilidade envolve a manutenção de um inventário de APIs preciso. Como acontece com a maioria das grandes organizações, o banco estava tendo dificuldades com APIs desconhecidas em seu ambiente. A realidade é: as empresas gerenciam milhares de APIs, muitas das quais não são direcionadas por meio de um proxy, como um gateway de APIs. Essas são chamadas de APIs não autorizadas ou APIs zumbis. Essas APIs provavelmente foram implantadas por ex-funcionários ou antes que a organização começasse a levar a sério a segurança de APIs. Seja qual for a razão pela qual elas existem, o gateway de APIs do banco não podia vê-las, então era fácil subestimar quantas APIs existiam.

Evoluir para atingir o desafio de segurança de APIs

A organização implantou a plataforma completa de segurança de APIs da Noname (agora parte do Akamai API Security), incluindo soluções de gerenciamento de postura de APIs, proteção de tempo de execução e testes no ambiente. A postura de segurança do cliente melhorou exponencialmente, pois agora ele é capaz de detectar e corrigir vulnerabilidades em um dos vetores de ameaças mais obscuros do mundo.

Agora, APIs desconhecidas podem ser descobertas e reveladas dentro da plataforma, permitindo visibilidade completa e mitigação de riscos. A instituição reduziu drasticamente a dispersão de APIs e melhorou a conformidade, já que o Akamai API Security classifica dados confidenciais para ajudar a satisfazer regulamentações como GDPR, HIPAA, entre outros.

O banco também agora tem a capacidade de interromper ataques em tempo real e proteger ativos de dados do cliente. A solução de proteção do tempo de execução detecta e prioriza ameaças potenciais, além de monitorar continuamente a atividade das APIs. Ao fazer a integração com firewalls de aplicativos da Web, gateways de APIs, gerenciamento de informações de segurança e eventos, gerenciamento de serviços de tecnologia da informação e outras ferramentas de fluxo de trabalho, nossa plataforma permite a correção de ameaças manualmente, semiautomaticamente ou automaticamente.

Resultados

As APIs se tornaram rapidamente o vetor de ataque preferido dos hackers, e não há sinais de desaceleração desses ataques. Por exemplo, vimos "um crescimento de 257% no número de ataques contra serviços financeiros ano após ano" em 2022. A empresa de serviços financeiros estará bem preparada para evitar se tornar parte da estatística e se defender contra essa tendência graças ao Akamai API Security. Em particular, as equipes de segurança dos clientes entenderão melhor os perigos que as APIs apresentam e poderão criar sistemas ainda mais seguros.