História do cliente da Akamai

Principal banco do EUA protege o tráfego de APIs e ganha visibilidade

Manutenção da conformidade regulatória rigorosa com visibilidade sem precedentes em sua superfície de ataques a APIs

O setor bancário passou por uma transformação significativa nos últimos anos, impulsionado pela adoção de APIs (interfaces de programação de aplicativos). Essa proliferação de APIs permitiu que os bancos aproveitassem novas oportunidades, melhorassem as experiências dos clientes e impulsionassem o crescimento dos negócios.

As APIs têm desempenhado um papel fundamental para permitir a integração perfeita entre diferentes sistemas e aplicativos dentro do ecossistema bancário. Ao expor seus serviços e dados por meio de APIs, os bancos agora podem colaborar com desenvolvedores terceirizados, startups de tecnologia financeira e outras instituições financeiras para criar soluções inovadoras e expandir suas ofertas. No entanto, apesar dessas vantagens claras, expor APIs sempre envolve algum risco.

Os riscos de segurança de APIs podem representar ameaças significativas à confidencialidade, integridade e disponibilidade de uma API. Esses riscos incluem acesso não autorizado, ataques por injeção, ataques de negação de serviço, transmissão de dados insegura, autorização insuficiente e escalonamento de privilégios, falta de validação de entrada, armazenamento de credenciais inseguro e registro e monitoramento inadequados. Para lidar com esses riscos, esse líder bancário estabeleceu relações com a Noname Security (agora uma empresa Akamai).

Manutenção da conformidade

No setor de serviços financeiros, o cumprimento das regulamentações é de extrema importância para garantir práticas justas e transparentes, proteger os clientes e manter a integridade do sistema financeiro. As regulamentações KYC (Conheça o seu cliente) e AML (Prevenção à

Banking Leader

Localização

Estados Unidos

Setor

Serviços financeiros

Solução

Akamai API Security

Principais impactos

- Conformidade regulatória fortalecida
- Integração com o ambiente de produção F5
- Identificação contínua de APIs

Akamai

lavagem de dinheiro) exigem que as instituições financeiras verifiquem a identidade de seus clientes, avaliem os riscos potenciais associados à lavagem de dinheiro e ao financiamento do terrorismo e relatem atividades suspeitas.

Outras regulamentações incluem o PCI DSS (Padrão de segurança de dados do setor de cartões de pagamento), que é um conjunto de padrões de segurança estabelecidos pelas principais empresas de cartões de crédito para proteger os dados dos titulares de cartões. Essas regulamentações são apenas a ponta do iceberg no que diz respeito às regulamentações financeiras. Por esse motivo, saber quais dados estão atravessando suas APIs era essencial para o líder de serviços financeiros.

A empresa precisava entender, gerenciar e mitigar os riscos melhorando a visibilidade geral de seu ecossistema de APIs, com ênfase na descoberta de APIs, classificação de dados, vulnerabilidade e detecção de anomalias. Também priorizou a integração com seu ambiente de produção F5.

Descoberta da sua pegada de APIs

A plataforma Noname API Security (agora parte da Akamai API Security) forneceu visibilidade sobre o tráfego de APIs transmitido de e para a rede do cliente, bem como dentro dela. O mecanismo do Akamai API Security analisou o tráfego e descobriu todas as APIs do líder de serviços financeiros. A análise de tráfego em tempo real identificou novas APIs e mudanças nas APIs existentes, e os dados foram registrados e atualizados no painel do cliente.

Como a plataforma não depende de agentes ou auxiliares, e porque se integra à infraestrutura de nuvem, ela vê todas as APIs, independentemente de estarem registradas em um gateway de APIs. Todas as APIs internas e externas, APIs legadas (aquelas que antecedem o gateway de APIs) e APIs sombra ou não autorizadas (aquelas que não são roteadas por meio de um gateway) foram descobertas, fornecendo ao cliente visibilidade sem precedentes na superfície de ataque a APIs.

Pensando no futuro

O líder bancário usa um conjunto de critérios para avaliar o sucesso de sua segurança de APIs. Um desses critérios, para os quais a Akamai está fornecendo suporte, é a triagem rápida. Um objetivo fundamental é determinar como analisar a gravidade de cada achado, o que permitiria que o SOC (Centro de operações de segurança) avaliasse, triasse e respondesse rapidamente a um alerta.

 | Publicado em 08/24