História do cliente da Akamai

Importante empresa de telecomunicações na Ásia protege APIs contra ameaças

A empresa ganhou visibilidade e proteção para todas as APIs em sua infraestrutura

Descobriu APIs não gerenciadas

Aprimorou a proteção à API

Protegeu dados confidenciais

O setor de telecomunicações em toda a Ásia está investindo fortemente no desenvolvimento de novas tecnologias e na expansão de redes para atender à demanda dos clientes por melhores serviços digitais à medida que os dispositivos móveis proliferam. Nos bastidores, as APIs fornecem:

- A conectividade necessária para a transformação do setor de telecomunicações, ao mesmo tempo em que acelera os processos das equipes de DevOps
- A base para entregar serviços de telefonia móvel, acesso à internet e outros produtos de telecomunicações aos clientes em todo o continente
- A capacidade de oferecer soluções mais personalizadas que culminassem na melhor experiência do cliente

Uma das principais empresas de telecomunicação da região também vê a grande oportunidade possibilitada pelas APIs, especificamente para oferecer novas soluções digitais de voz e dados. E, à medida que a era 5G se aproxima, a empresa voltou sua atenção para além da telefonia e em direção ao big data, IA, IoT e outras aplicações digitais emergentes. No entanto, ela também entende que as APIs estão proliferando não apenas em número, mas em risco. Tendo presenciado outros grandes provedores de telecomunicações sofrerem os efeitos dos ataques a APIs em 2022 e 2023, a empresa recorreu à Noname Security (agora uma empresa Akamai).

Telecommunications Company

Localização

Ásia

Setor

Operadora de rede

Solução

Akamai API Security

Akamai

Necessidade de visibilidade de todas as APIs e seus riscos

Como acontece com muitas organizações, a falta de visibilidade das APIs e seus riscos é um desafio prevalente para as equipes de segurança. De acordo com nossa pesquisa, apenas 4 em cada 10 organizações com inventários de API completos sabem qual das suas APIs retornam dados confidenciais. Ao usar o módulo de descoberta da nossa solução de segurança de APIs, determinamos que nosso cliente de telecomunicações estava enfrentando um desafio semelhante.

Antes de trabalhar com a Akamai, os controles de segurança de APIs do cliente consistiam principalmente em uma plataforma de gerenciamento de APIs legada e WAF (firewall de aplicativos da Web). A partir de uma perspectiva de segurança de aplicativos e entrega de APIs, esse acordo fazia sentido. No entanto, nenhuma solução oferecia o alto grau de controles de segurança e observabilidade necessários para proteger de forma abrangente as APIs dos métodos de ataque atuais. Uma razão-chave: nem todas as APIs eram direcionadas por meio de um proxy como um WAF ou gateway de APIs, e essas APIs não gerenciadas são alvos atrativos para agentes mal-intencionados.

Mas, mesmo com uma auditoria precisa do inventário de APIs, a empresa ainda precisava de recursos para proteger as APIs durante seu funcionamento normal à medida que operavam e gerenciavam solicitações. De forma bem simples, seria impossível para a equipe de segurança de uma organização identificar manualmente o comportamento mal-intencionado em seu ambiente.

Existem centenas, se não milhares, de pontos de extremidade de APIs que precisam ser protegidos em tempo real. As soluções de AppSec comumente usadas normalmente não podem acompanhar todas as chamadas de API no ambiente de um cliente, e isso pode deixar o ambiente de TI de uma empresa vulnerável a ataques cibernéticos sem os recursos adequados de proteção de tempo de execução de APIs.

Soluções para ver todas as APIs e se proteger contra ameaças a APIs

A primeira fase do engajamento implicou uma implantação piloto para localizar as APIs internas da empresa, avaliar configurações e entender os tipos de dados que passam pelas APIs. O cliente ficou imediatamente impressionado com a velocidade em que a descoberta foi executada, as descobertas precisas do inventário e a exposição de dados confidenciais que a ferramenta identificou.

Devido aos resultados positivos do piloto, o cliente expandiu a área de cobertura da plataforma de segurança de APIs da Noname (agora parte do Akamai API Security) para toda a sua infraestrutura de APIs interna e externa. Esse exercício também revelou APIs de produção mais ocultas e descobriu as ameaças mais iminentes ao ambiente.

Descobrimos que o cliente precisava de uma defesa mais forte contra grandes vulnerabilidades de segurança para proteger suas APIs contra futuros ataques. Com o Akamai API Security implantado, o cliente agora pode detectar anomalias comportamentais suspeitas e acionar protocolos de resposta a incidentes em tempo real. Isso ajuda uma organização a evitar ter que confiar em relatórios atrasados e registros de acesso para embasar seu processo de correção. Depois que comportamentos suspeitos são detectados com o Akamai API Security, eles são reportados ao gateway de APIs do cliente, sistema SIEM e outros mecanismos de segurança da informação para informar toda a equipe de segurança. O cliente pode escolher fazer com que a equipe corrija os problemas manualmente, semiautomaticamente ou totalmente automaticamente, dependendo do caso de uso e gravidade da vulnerabilidade.

| Publicado em 09/24