Témoignage de client d'Akamai

Une grande banque américaine sécurise le trafic des API et gagne en visibilité

Maintenir une conformité réglementaire stricte avec une visibilité sans précédent sur la surface d'attaque des API

Le secteur bancaire a connu une transformation importante ces dernières années, stimulée par l'adoption d'interfaces de programmation d'applications (API). Cette prolifération des API a permis aux banques de tirer parti de nouvelles opportunités, d'améliorer l'expérience client et de stimuler la croissance de l'activité.

Les API ont joué un rôle crucial en permettant une intégration fluide entre les différents systèmes et applications au sein de l'écosystème bancaire. En exposant leurs services et leurs données via des API, les banques peuvent désormais collaborer avec des développeurs tiers, des start-ups fintech et d'autres établissements financiers pour créer des solutions innovantes et élargir leurs offres. Cependant, malgré ces avantages évidents, l'exposition des API n'est pas sans risque.

Les risques liés à la sécurité des API peuvent constituer des menaces importantes pour la confidentialité, l'intégrité et la disponibilité d'une API. Ces risques incluent l'accès non autorisé, les attaques par injection, les attaques par déni de service, la transmission de données non sécurisée, l'autorisation insuffisante et l'escalade des privilèges, l'absence d'Input Validation, le stockage non sécurisé des informations d'identification, ainsi que la journalisation et la surveillance inadéquates. Pour faire face à ces risques, ce leader des services bancaires a fait appel à Noname Security (désormais une entreprise Akamai).

Maintien de la conformité

Dans le secteur des services financiers, le respect des réglementations est de la plus haute importance pour assurer des pratiques équitables et transparentes, protéger les utilisateurs et maintenir l'intégrité du système financier. Les réglementations en matière de connaissance des clients

Banking Leader

Localisation

États-Unis

Secteur

Services financiers

Solution

Akamai API Security

Impacts majeurs

- Renforcement de la conformité réglementaire
- Intégration à l'environnement de production F5
- Identification API continue

Akamai

(Know Your Customer, KYC) et d'anti-blanchiment d'argent (Anti-Money Laundering, AML) exigent que les établissements financiers vérifient l'identité de leurs clients, évaluent les risques potentiels associés au blanchiment d'argent et au financement du terrorisme, et signalent les activités suspectes.

Parmi les autres réglementations, figure la norme de sécurité de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard ou PCI DSS), qui est un ensemble de normes de sécurité établies par les principales sociétés de cartes de crédit pour protéger les données des titulaires de carte. Ces réglementations ne sont que la partie visible de l'iceberg en matière de réglementation financière. Il était donc crucial pour le leader des services financiers de savoir quelles données transitent par ses API.

L'entreprise avait besoin de comprendre, gérer et atténuer les risques en améliorant la visibilité globale de son écosystème d'API, en mettant l'accent sur la détection des API, la classification des données, la détection des vulnérabilités et des anomalies. Elle devait également privilégier l'intégration avec son environnement de production F5.

Détection de l'empreinte API

La plateforme Noname de sécurité des API (désormais intégrée à Akamai API Security) a fourni une visibilité sur le trafic des API transmis depuis et vers le réseau du client, ainsi qu'au sein de ce réseau. Le moteur Akamai API Security a analysé le trafic et détecté toutes les API du leader des services financiers. L'analyse du trafic en temps réel a permis d'identifier de nouvelles API et des modifications apportées aux API existantes. Par ailleurs, les données ont été enregistrées et mises à jour dans le tableau de bord du client.

Étant donné que la plateforme ne repose pas sur des agents ou des extensions, et qu'elle s'intègre à l'infrastructure cloud, elle détecte chaque API, qu'elle soit enregistrée ou non auprès d'une passerelle d'API. Des API internes et externes, d'anciennes API (antérieures à la passerelle d'API) et des API fantômes ou malveillantes (non acheminées via une passerelle) ont toutes été découvertes, offrant au client une visibilité sans précédent sur la surface d'attaque des API.

Perspectives d'avenir

Le leader des services bancaires utilise un ensemble de critères pour évaluer la sécurité de ses API. L'un d'entre eux, pris en charge par Akamai, est le triage rapide. L'objectif principal est de déterminer comment analyser la gravité de chaque résultat, ce qui permet au centre d'opérations de sécurité (SOC) d'évaluer et de trier rapidement les alertes, puis d'y répondre sans délai.

 | Publication 08/24