Témoignage de client d'Akamai

Une société financière détecte et sécurise les API

Une banque a protégé ses initiatives digitales en détectant des API cachées, en évaluant et en atténuant les risques liés aux API et en répondant aux exigences réglementaires

Visibilité totale

Amélioration de la sécurité

Sécurisation des initiatives digitales

Le secteur des services financiers adopte rapidement la transformation digitale pour rester compétitif sur un marché en constante évolution. En utilisant des capacités digitales telles que l'intelligence artificielle et l'analyse de Big Data, les institutions financières sont en mesure d'offrir des produits innovants, de réduire les coûts et de fournir des services plus personnalisés et efficaces à leurs clients.

Mais la transformation digitale s'accompagne d'un risque accru de cyberattaques. Pour lutter contre ce problème croissant, la cybersécurité joue aujourd'hui un rôle essentiel dans toute stratégie de transformation digitale. Les entreprises de services financiers doivent s'assurer que leurs systèmes sont sécurisés et résilients pour protéger les données et les actifs de leurs clients contre les acteurs malveillants.

L'une des principales banques commerciales asiatiques a rapidement fait appel à Noname Security (désormais une entreprise Akamai) pour l'aider à renforcer sa sécurité des API. Les violations d'API se sont développées à un rythme alarmant ; selon Tech Wire Asia, « à l'heure actuelle, 1 cyber-incident sur 13 peut être attribué au manque de sécurité des API ». Le site Web souligne également que « les vulnérabilités des API coûtent aux entreprises jusqu'à 75 milliards de dollars par an ».

Étant donné que notre client possède au total plus de 700 milliards de dollars d'actifs, quelque 5 000 clients professionnels et une réputation de gestion de patrimoine de renommée internationale, il était impératif que toutes les vulnérabilités des API soient corrigées dès que possible.

Financial Services

Localisation

Asie

Secteur

Services financiers

Solution

Akamai API Security

Akamai

La nécessité d'une meilleure visibilité sur les API et leurs risques

L'institution avait déjà déployé une plateforme de gestion des API pour l'authentification et le contrôle du trafic, mais il existait des doutes quant à sa capacité à prévenir les abus d'API et les cyberattaques. Bien que les passerelles d'API fournissent des contrôles de base de sécurité des API indispensables, elles ne sont malheureusement pas suffisantes pour protéger correctement les entreprises contre les menaces propres aux API.

Par exemple, la Broken Object Level Authorization, souvent appelée BOLA, apparaît comme un trafic d'API normal vers les passerelles. Ce manque de perception contextuelle entre les requêtes et les réponses des API permet aux attaques BOLA d'accéder aux services back-end critiques sans être détectées. En plus de rendre les entreprises vulnérables aux défaillances de la BOLA, cette faille risque d'ouvrir la porte à d'autres attaques et abus de logique métier.

Pour pallier aux problèmes de visibilité, il est également nécessaire de tenir un inventaire des API précis. Comme la plupart des grandes entreprises, la banque se heurtait à des API inconnues présentes dans son environnement. La réalité est que les entreprises gèrent des milliers d'API, dont beaucoup ne sont pas acheminées via un proxy tel qu'une passerelle d'API. On les appelle « API malveillantes » ou « API zombies ». Ces API ont probablement été déployées par d'anciens employés ou avant que l'entreprise ne prenne au sérieux la sécurité des API. Quelle que soit leur raison d'exister, la passerelle d'API de la banque était incapable de les voir, il était donc devenu facile de sous-estimer leur nombre.

Relever le défi de la sécurité des API

L'entreprise a déployé la plateforme complète Noname de sécurité des API (désormais intégrée à Akamai API Security), qui comprend des solutions de gestion de la posture des API, de protection de l'exécution et de tests dans l'ensemble de son environnement. La posture de sécurité du client s'est améliorée de manière exponentielle, car ce dernier est désormais en mesure de détecter et de corriger les vulnérabilités de l'un des vecteurs de menaces les plus obscurs au monde.

Désormais, les API inconnues peuvent être identifiées et révélées au sein de la plateforme, offrant une visibilité complète et une atténuation des risques. L'institution financière a considérablement réduit la prolifération de ses API et amélioré la conformité, car Akamai API Security classifie les données sensibles afin de satisfaire aux réglementations telles que le RGPD, l'HIPAA, etc.

En outre, la banque a désormais la possibilité de bloquer les attaques en temps réel et de protéger les données de ses clients. La solution de protection de l'exécution détecte et hiérarchise intelligemment les menaces potentielles tout en surveillant en permanence l'activité des API. En s'intégrant aux pare-feux d'application Web, aux passerelles d'API, à la gestion des informations de sécurité et des événements, à la gestion des services de technologie de l'information et à d'autres outils de flux de travail, notre plateforme permet de corriger les menaces manuellement, semi-automatiquement ou automatiquement.

Résultats

Les API sont rapidement devenues un vecteur d'attaque privilégié pour les pirates, et les attaques ne montrent aucun signe de ralentissement. Par exemple, nous avons constaté « une croissance de 257 % du nombre d'attaques contre les services financiers d'une année sur l'autre » en 2022. Grâce à Akamai API Security, la société de services financiers sera bien équipée pour se défendre contre cette tendance et éviter de grossir les statistiques. Les équipes de sécurité du client auront notamment une meilleure compréhension des dangers que présentent les API et seront en mesure de créer des systèmes encore plus sécurisés.

| Publication 08/24