Témoignage de client d'Akamai

Un leader du secteur des télécommunications asiatique protège les API contre les menaces

L'entreprise a gagné en visibilité — et en protection — pour chaque API de son parc

Détection des API non gérées

Protection des API améliorée

Sécurisation des données sensibles

Dans un contexte de multiplication des terminaux mobiles, le secteur des télécommunications asiatique investit massivement dans le développement de nouvelles technologies et l'expansion des réseaux afin de répondre aux demandes de meilleurs services digitaux exprimées par les clients. En coulisse, les API fournissent :

- la connectivité nécessaire à la transformation du secteur des télécommunications tout en accélérant les processus des équipes DevOps ;
- la base permettant de fournir des services de téléphonie mobile, un accès à Internet et d'autres produits de télécommunication aux clients du continent ;
- la capacité d'offrir des solutions plus personnalisées et d'améliorer l'expérience client.

L'un des principaux opérateurs de télécommunications de la région voit également la grande opportunité que représentent les API, notamment pour offrir de nouvelles solutions voix et données digitales. Et à l'approche de l'ère de la 5G, l'entreprise voit au-delà de la téléphonie et se tourne vers le Big Data, l'IA, l'IoT et d'autres applications digitales émergentes. Elle est toutefois consciente que la multiplication des API s'accompagne d'une augmentation des risques. Après avoir vu d'autres grands fournisseurs de télécommunications subir les conséquences d'attaques d'API en 2022 et 2023, la société a fait appel à Noname Security (désormais une entreprise Akamai).

Telecommunications Company

Localisation

Asie

Secteur

Opérateur réseau

Solution

Akamai API Security

Akamai

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

Comme dans de nombreuses entreprises, le manque de visibilité sur les API et leurs risques représente un défi majeur pour les équipes de sécurité. Selon nos études, seules 4 entreprises sur 10 disposant d'inventaires d'API complets savent lesquelles de leurs API renvoient des données sensibles. En utilisant le module Discovery de notre solution de sécurité des API, nous avons déterminé que notre client du secteur des télécommunication était confronté à un défi similaire.

Avant de travailler avec Akamai, les contrôles de sécurité des API du client consistaient principalement en une plateforme de gestion des API héritée et un pare-feu d'application Web (WAF). Du point de vue de la sécurité des applications et de la diffusion des API, cette configuration était logique. Mais aucune des deux solutions n'offre le niveau élevé de contrôles de sécurité et d'observabilité nécessaire à la fourniture d'une protection complète des API contre les méthodes d'attaque actuelles. Et ce pour une raison principale : toutes les API ne sont pas acheminées via un proxy tel qu'un WAF ou une passerelle d'API, et ces API non gérées sont des cibles attrayantes pour les acteurs malveillants.

Un audit précis de l'inventaire d'API ne suffisait pas : l'entreprise avait également besoin de capacités pour sécuriser les API pendant leurs opérations normales d'exploitation et de gestion des requêtes. Il serait tout bonnement impossible pour l'équipe de sécurité d'une entreprise d'identifier manuellement les comportements malveillants dans son environnement.

Il existe des centaines, voire des milliers, de points de terminaison d'API qui doivent être protégés en temps réel. Les solutions AppSec couramment utilisées ne peuvent généralement pas suivre chaque appel d'API dans l'environnement d'un client, ce qui rend l'environnement informatique d'une entreprise vulnérable aux cyberattaques si elle ne dispose pas des capacités de protection de l'exécution des API appropriées.

Solutions pour voir toutes les API et se protéger contre les menaces qui leur sont liées

La première phase de la collaboration comprenait un déploiement pilote visant à localiser les API internes de l'entreprise, évaluer les configurations et comprendre les types de données transitant par les API. Le client a immédiatement été impressionné par la rapidité de détection, les résultats précis de l'inventaire et l'exposition des données sensibles identifiées par l'outil.

Suite aux résultats positifs du pilote, le client a ensuite étendu la zone de couverture de la plateforme Noname de sécurité des API (désormais intégrée à Akamai API Security) à l'ensemble de son parc d'API interne et externe. Cet exercice a révélé d'autres API de production cachées et a mis à jour les menaces les plus imminentes pour l'environnement.

Nous avons constaté que le client avait besoin d'une défense renforcée contre les principales vulnérabilités de sécurité pour protéger ses API contre de futures attaques. Grâce au déploiement d'Akamai API Security, le client peut désormais détecter les anomalies comportementales suspectes et déclencher des protocoles de réponse aux incidents — en temps réel. Cela permet à l'entreprise d'éviter de dépendre de la réception retardée des rapports et des journaux d'accès pour informer son processus de correction. Une fois les comportements suspects détectés grâce à Akamai API Security, ils sont signalés à la passerelle d'API du client, au système SIEM et à d'autres moteurs de sécurité de l'information afin d'en informer l'ensemble de l'équipe de sécurité. Le client peut choisir de demander à son personnel de corriger le ou les problèmes manuellement, semi-automatiquement ou entièrement automatiquement, en fonction du cas d'utilisation et de la gravité de la vulnérabilité.