Témoignage de client d'Akamai

Un distributeur de boissons figurant au classement Fortune 100 sécurise ses API et ses données

Protection des données client en identifiant les principales vulnérabilités des API et en réparant les dommages causés par les fraudes, abus et vols antérieurs

Les interfaces de programmation d'applications, ou API, permettent aux détaillants de créer des expériences personnalisées de bout en bout pour les clients, tout en rationalisant les opérations. Chaque variable qui place une boisson entre les mains des consommateurs, y compris les données d'inventaire, les soumissions de commandes, les données de localisation, les paiements et même les programmes de récompenses, est fournie par des API. Les API ont révolutionné l'expérience d'achat en connectant l'écosystème des détaillants, de leurs partenaires et de leurs clients. Mais leur proximité constante avec des données sensibles présente également un risque.

Même si les consommateurs apprécient la nouvelle expérience de commerce de détail digital, ils sont souvent préoccupés par la protection de leurs informations personnelles, et à juste titre. Les API deviennent de plus en plus un vecteur d'attaque privilégié par les cybercriminels. Voilà pourquoi une entreprise de distribution de boissons du classement Fortune 100 a fait appel à Noname Security (désormais une entreprise Akamai) pour corriger les vulnérabilités de sa posture de sécurité des API.

Les défis d'une empreinte API toujours plus forte

Lors de nos premières conversations, l'entreprise a exprimé des inquiétudes quant à son incapacité à mettre en place une gouvernance et une sécurité des API pertinentes à l'échelle mondiale. Pour confirmer ses doutes, elle a commandé une chasse aux bugs accessible au grand public. Cette analyse a révélé une énorme

Retail Beverage Company

Localisation

États-Unis

Secteur

Commerce de détail, tourisme et hôtellerie

Solution

Akamai API Security

Impacts majeurs

- Protection de plus d'un milliard d'appels d'API par jour
- Sécurisation de 5 000 requêtes par seconde
- Identification et résolution de plus de 200 problèmes

Akamai

vulnérabilité : les noms, adresses, e-mails et numéros de téléphone de près de 100 millions d'utilisateurs auraient pu être exfiltrés. Fort heureusement, il s'agissait simplement de la conclusion de la recherche de bugs, et les problèmes ont été corrigés sans préjudice.

Par ailleurs, la visibilité et la surveillance des API de production de l'entreprise étaient insuffisantes, ce qui l'empêchait d'évaluer correctement les risques, et ses données Apigee ne fournissaient pas de détails contextuels (par exemple, types de données, comportement des utilisateurs, bases de référence, analyse des vulnérabilités). En raison de ces vulnérabilités des API, des fraudes, des abus et des vols ont été commis. Ces méfaits se sont traduits par des coûts d'exploitation élevés pour le détaillant.

Renforcer la posture de sécurité des API

La plateforme Noname de sécurité des API (désormais intégrée à Akamai API Security) a pu inventorier les API du client et fournir une analyse comportementale, une détection des attaques en temps réel et une gestion des failles de sécurité, y compris des tests AppDev spécifiques aux API. Le client a donc pu détecter et corriger les attaques d'API qui n'avaient pas été décelées par les contrôles existants. L'équipe de sécurité des applications, ou AppSec, a été en mesure d'accroître l'efficacité et d'améliorer la hiérarchisation des problèmes à haut risque.

Akamai prend également en charge jusqu'à 50 000 API par moteur, sans latence opérationnelle. En utilisant notre plateforme comme technologie de base, le client a développé un programme mondial de sécurité des API. Il bénéficie désormais d'une visibilité complète sur son inventaire d'API, avec des détails pertinents sur le plan contextuel. En outre, l'entreprise a pu recueillir des renseignements précieux qui n'étaient pas disponibles avec les outils existants. Elle dispose ainsi de capacités puissantes à moindre coût pour une gestion efficace des failles de sécurité des API et une détection des menaces en temps réel.

 | Publication 08/24