Témoignage de client d'Akamai

Un détaillant du classement Fortune 100 protège ses activités digitales avec API Security

Se conformer aux réglementations clés et éradiquer les attaques DDoS potentielles et les fuites de données

Le commerce de détail subit une transformation importante avec l'adoption de processus digitaux, stimulée par la puissance des interfaces de programmation d'applications (API). Les API révolutionnent la manière dont les détaillants opèrent, interagissent avec les clients et gèrent leurs activités.

Les détaillants intègrent leurs systèmes à divers services et applications tiers via des API, ce qui permet des interactions fluides sur différentes plateformes. Par exemple, les API permettent aux détaillants d'intégrer leurs plateformes de commerce électronique à des passerelles de paiement, des prestataires de transport et des systèmes de gestion des stocks. Cependant, à mesure que cet écosystème évolue, il génère une multitude de vulnérabilités potentielles en matière de sécurité.

La sécurité des API est primordiale dans l'écosystème digital actuel. Alors que les entreprises s'appuient de plus en plus sur les API pour connecter les systèmes, partager des données et permettre des intégrations, il devient essentiel de garantir la sécurité de ces interfaces. Voilà pourquoi ce détaillant du classement Fortune 100 s'est tourné vers Noname Security (désormais une entreprise Akamai) pour sécuriser la surface d'attaque de ses API.

Détecter la surface d'attaque des API

La détection des API joue un rôle crucial dans le contrôle de la prolifération des API, autrement dit la multiplication incontrôlée des API au sein d'une entreprise. Alors que les entreprises adoptent de plus en plus les API pour accompagner leur transformation digitale et stimuler l'innovation, il devient essentiel d'avoir une approche systématique pour détecter et gérer efficacement ces API. De plus, dans la mesure où l'écosystème du commerce de détail digital est en pleine croissance, il s'agit d'une première étape cruciale pour garantir la protection de vos API.

Designer Merchandise Retailer

Localisation

États-Unis

Secteur

Commerce de détail

Solution

Akamai API Security

Impacts majeurs

- Exposition des données évitée
- Détection de la surface d'attaque des API
- Réduction des risques et des coûts

Akamai

Ce leader du commerce de détail était confronté à un manque de visibilité en matière d'inventaire et de trafic d'API. Sans gouvernance sur des plateformes disparates (sur site et dans le cloud), l'entreprise n'était pas en mesure de développer une protection SDLC évolutive pour ses API. L'entreprise s'est engagée à fournir une détection continue des ressources API afin de réduire les risques et les coûts en identifiant les erreurs de configuration, les vulnérabilités et les non-conformités, et de l'intégrer à son flux de production SecOps existant (par exemple, Splunk).

Prévenir l'exposition des données sensibles

Dans le secteur du commerce de détail, il existe plusieurs réglementations de conformité auxquelles les entreprises doivent se conformer. Ces réglementations visent à protéger les droits des consommateurs, à garantir des pratiques commerciales équitables et à préserver la confidentialité et la sécurité des données. Les entreprises doivent être en mesure d'identifier et de sécuriser les API qui traitent des données sensibles afin de se conformer aux réglementations clés et aux normes du secteur, et ainsi éviter les conséquences juridiques et les atteintes à la réputation.

L'équipe d'Akamai a aidé le détaillant du classement Fortune 100 à empêcher que les données sensibles ne soient divulguées publiquement. Le détaillant utilisait une ancienne version de Jira, ce qui provoquait un bug exposant publiquement les noms des employés, les noms d'utilisateur Jira et les adresses e-mail. Les API exposées au public présentaient également un risque de posture de sécurité.

Pour l'entreprise, la solution Akamai API Security a pu combler les lacunes de la posture de sécurité des API et corriger les erreurs de configuration dans son environnement. Par exemple, la mauvaise configuration de l'architecture a ouvert la voie à des risques accrus via les attaques DDoS et les fuites de données.

Perspectives d'avenir

Le client collabore activement avec l'équipe Akamai chaque semaine pour favoriser l'adoption de la solution par son entreprise. Il est également impatient de découvrir de nouvelles intégrations avec ses flux de travail existants. Akamai API Security identifie et hiérarchise intelligemment les vulnérabilités potentielles, qui peuvent être corrigées manuellement, semi-automatiquement ou entièrement automatiquement par le biais d'intégrations dans des WAF, des passerelles d'API, des SIEM, des ITSM, des outils de flux de travail ou d'autres services. Par ailleurs, étant donné la croissance rapide de la pile technologique du client, un certain nombre d'intégrations sont en cours de révision.

| Publication 08/24