Témoignage de client d'Akamai

Une entreprise de sport et médias détecte les risques cachés liés aux API

Établissement d'un inventaire complet des API et identification des erreurs de configuration qui ouvrent la porte aux attaques d'API

Établissement d'un inventaire précis

Détection de contrôles manquants

Découverte d'une attaque par injection SQL

Les plateformes et les applications digitales révolutionnent l'industrie du sport et des médias grâce à la puissance des API. Ces avancées technologiques transforment la façon dont les événements en live sont organisés, promus et vécus, créant de nouvelles opportunités pour les artistes, les organisateurs d'événements et les audiences.

Les API peuvent partager en toute fluidité des informations sur les événements, des mises à jour et des liens d'achat de billets sur divers réseaux sociaux, ce qui permet d'augmenter la visibilité et de booster les ventes de tickets. De plus, les API transforment l'expérience sur site lors d'événements en live. L'intégration avec les applications pour mobile et les terminaux portables offre des fonctionnalités interactives telles que des programmes personnalisés, des cartes interactives et des notifications en temps réel.

Il est toutefois important de noter que la nature sensible des données et des transactions impliquées dans le secteur du sport et des médias impose de donner la priorité à la sécurité des API. Les contrôles de sécurité des API jouent un rôle essentiel pour garantir l'intégrité, la confidentialité et la disponibilité des données, ce qui explique pourquoi cette entreprise de sport et médias de renommée mondiale a fait appel à Noname Security (désormais une entreprise Akamai).

Adoption de la sécurité des API

Le client était bien conscient de la nécessité de sécuriser les API, mais il ne savait pas exactement par où commencer et quels domaines privilégier. Traditionnellement, il s'était principalement concentré sur la sécurité des applications et estimait que ses outils existants, tels que les passerelles d'API et les pare-feux d'application Web suffiraient à protéger

Sports and Media Company

Localisation

États-Unis

Secteur

Média et divertissement

Solution

Akamai API Security

Akamai

les API. Mais bien que ces outils puissent offrir certaines protections de base, ils ne sont pas conçus pour fournir le même degré de visibilité, de sécurité en temps réel et de tests continus que les solutions spécialisées de sécurité des API. Il était impossible de fournir la plupart de ces protections avec l'infrastructure actuelle du client. Par exemple, deux des aspects clés de la sécurité des API sont l'authentification et l'autorisation. Les mécanismes d'authentification appropriés garantissent que seuls les utilisateurs ou systèmes autorisés peuvent accéder aux API.

Détection des vulnérabilités

L'équipe Akamai API Security a utilisé ses modules Posture Management et Runtime Protection pour comprendre la posture de sécurité des API actuelles du client. Après avoir dressé un inventaire précis des API dans l'environnement du client, nous avons pu détecter les failles de sécurité et les erreurs de configuration existantes.

Nous avons tout d'abord découvert que le client était victime d'une attaque par injection SQL (SQLi). Une SQLi est un type de vulnérabilité de sécurité qui se produit lorsqu'un attaquant peut manipuler les paramètres d'entrée d'une requête API pour exécuter des commandes SQL non autorisées. Les conséquences d'une attaque SQLi réussie peuvent être graves. Les attaquants peuvent obtenir un accès non autorisé à des données sensibles, modifier ou supprimer des données, ou même exécuter des commandes arbitraires sur le serveur de base de données sous-jacent.

Nous avons ensuite découvert que le système d'authentification du client était défaillant. Sans une authentification appropriée, n'importe qui peut accéder aux points de terminaison d'API et potentiellement récupérer ou modifier des données sensibles. Les attaquants peuvent modifier ou supprimer des données, entraînant des problèmes d'intégrité des données et une perte potentielle d'informations critiques. Il existe un risque de violation de données, de divulgation non autorisée d'informations voire de compromission complète du système.

Perspectives d'avenir

Maintenant que le client contrôle ses API en production, il cherche comment corriger les vulnérabilités avant la production. Pour aider les entreprises à identifier ces vulnérabilités et à y remédier, Akamai API Security inclut Active Testing, une solution de tests de sécurité des API spécialement conçue pour comprendre la logique métier unique d'une entreprise et fournir une couverture complète de ses vulnérabilités spécifiques aux API. Active Testing aide les entreprises à adopter une approche « shift left » et à intégrer les tests de sécurité des API à chaque phase de développement.

 | Publication 09/24