Akamai-Kundenreferenz

API Security integriert Reise-API für Dan Hotels

Die Luxushotelkette mit Hotels in ganz Israel und Indien setzt auf API Security, um ihre zahlreichen API-Integrationen in der Reisebranche zu schützen

Einfacheres Management | Erweiterte Transparenz | Geringere Workload

APIs schützen – eine Herausforderung

Die Kette Dan Hotels verfügt über viele verschiedene API-basierte Integrationen, die das interne Business-Intelligence-System unterstützen, sowie eine wachsende Sammlung externer APIs mit Partnern aus der Reisebranche. Darunter sind große Reise-Websites wie Expedia und Booking.com, Online-Reisebüros und verschiedene andere Anbieter und kleinere Agenten. Viele dieser API-Funktionen sind in der Silverbyte Property Management-Plattform des Unternehmens zentralisiert. Das Sicherheitsteam stellte jedoch fest, dass es in Bezug darauf, wie Partner auf seine Systeme zugreifen oder mit ihnen interagieren, an Transparenz fehlte – und die Fähigkeit, diese Aktivitäten zu steuern. Nachdem zwei Reisepartner des Unternehmens gefährdet worden waren, entschied das Team, dass ein umfassender und proaktiver Ansatz für die API-Sicherheit erforderlich war. „Als wir den Vorfall mit unseren Partnern untersuchten, erkannten wir, wie wenig Kontrolle wir über die Nutzung unserer APIs haben. Uns wurde klar, dass nicht besonders sichere Partner unsere Systeme gefährden könnten“, so Yossi Gabay, Vice President of Information Systems, Dan Hotels. Diese Erfahrung hat dem Unternehmen

Dan Hotels

Tel Aviv, Israel
danhotels.com

Branche

Gastgewerbe

Lösung

API Security

 | Veröffentlicht: 08/23

gezeigt, dass es dringend notwendig war, eine Reihe komplexerer API-Sicherheitsfunktionen zu implementieren.

Erfolgsfaktoren sicherer APIs

Das Technologieteam von Dan Hotels steht täglich unter großem Konkurrenzdruck, der Cybersicherheit und andere kritische Betriebsfunktionen umfasst. Aus diesem Grund musste eine Lösung her, die das API-Risiko reduzieren würde, ohne das Team mit Störungen und manuellem Aufwand zu überfordern. Wichtig war auch, dass der Ansatz über offensichtliche Angriffe hinausgeht und nuanciertere Formen des API-Missbrauchs abdeckt, der von Partnern ausgeht.

Warum Dan Hotels sich für API Security entschieden hat

Dank des SaaS-Modells (Software as a Service) von API Security (vormals Neosec) konnte Dan Hotels die erste Implementierung innerhalb weniger Stunden durchführen. „Die Integration war einfach und verlief reibungslos“, so Gabay. „Wir waren nicht mit neuen Aufgaben überlastet, der tägliche Betriebs wurde nicht beeinträchtigt.“ Sobald das System betriebsbereit war, arbeitete das API-Security-Team mit dem Team von Dan Hotels zusammen, um die Datenquellen und die Konfiguration so zu optimieren, dass sie den einzigartigen Zielen des Unternehmens entsprechen.

Da sich das Unternehmen auf das Erkennen von Missbrauch konzentriert, unterscheidet sich API Security durch die verhaltensanalytischen Funktionen von anderen Optionen auf dem Markt. Die API-Security-Plattform konnte die Beziehungen zwischen den API-Nutzern und -Ressourcen der Hotelkette zuordnen und so einen wertvollen Kontext liefern. „API Security hat sich nicht nur auf das Blockieren von Angriffen konzentriert, sondern konnte uns dabei helfen nachzuvollziehen, was tatsächlich passiert ist. Wir können uns auf unerwünschtes Verhalten fokussieren, das ansonsten unbemerkt bleiben würde“, so Gabay.

> API Security kombiniert Erkennungsfunktionen mit Threat Hunting. Es vereint somit alle Erkenntnisse, die wir zur Risikominimierung benötigen, an einem zentralen Ort und schafft einen erheblichen Mehrwert für unser Unternehmen.
>
> **– Yossi Gabay**
> *VP of Information Systems, Dan Hotels*

Das Team von Dan Hotels war auch sehr davon beeindruckt, wie API Security, große Mengen an Informationen über API-Aktivitäten und -Bedrohungen in einer intuitiven, zeitbasierten Ansicht darzustellen vermag. „Ohne die relevanten Informationen kann man nicht darüber sprechen oder es in Ordnung bringen“, erklärt Gabay. „Sobald man versteht, was eine API tun soll und wie das im Vergleich zu den tatsächlichen Vorgängen aussieht, kann man alle relevanten Parteien einbeziehen, um Probleme zu beheben.“

Dan Hotels verfügt zwar über unternehmensinterne Sicherheitskenntnisse, sieht jedoch einen erheblichen Wert im Managed Threat Hunting Service von API Security. „Unser Team konzentriert sich gleichzeitig auf Cybersicherheit und die Unterstützung wertschöpfender Aktivitäten. Daher ist es für uns sehr wichtig, einen Managed Service in Anspruch nehmen zu können, der uns proaktiv warnt, wenn neue API-Risiken erkannt werden“, so Gabay. „So erhalten wir Zugang zu Experten, die in diesen API-Sicherheitsfragen auf dem neuesten Stand sowie sehr engagiert sind und eine einfache Zusammenarbeit ermöglichen.“

Dan Hotels ist eine Luxushotelkette mit Sitz in Israel. Das Unternehmen verwaltet über 4.000 Zimmer in 18 Hotels in Israel und Indien sowie eine vielfältige Auswahl an anderen Hotelangeboten wie Flughafen-Lounges und Catering.

danhotels.com

 | Veröffentlicht: 08/23