Akamai-Kundenreferenz

Führender Telekommunikationsanbieter in Asien sichert APIs gegen Bedrohungen ab

Das Unternehmen erhielt Einblick in jede API in seinem Bestand und konnte diese schützen

Erkennung nicht verwalteter APIs

Verbesserung des API-Schutzes

Sicherung sensibler Daten

Die Telekommunikationsbranche in ganz Asien investiert massiv in die Entwicklung neuer Technologien und den Ausbau von Netzwerken, um der Kundennachfrage nach besseren digitalen Diensten gerecht zu werden, da mobile Geräte immer beliebter werden. Hinter den Kulissen bieten APIs:

- die notwendige Konnektivität für die Transformation der Telekommunikationsbranche und beschleunigen gleichzeitig die Prozesse der DevOps-Teams
- die Grundlage für die Bereitstellung von Mobilfunkdiensten, Internetzugang und anderen Telekommunikationsprodukten für Kunden auf dem gesamten Kontinent
- die Möglichkeit, stärker personalisierte Lösungen anzubieten und letztlich das Kundenerlebnis zu verbessern

Eines der führenden Telekommunikationsunternehmen der Region sieht in APIs außerdem eine große Chance – insbesondere für das Angebot neuer digitaler Sprach- und Datenlösungen. Und während die 5G-Ära näher rückt, hat das Unternehmen seinen Blick über die Telefonie hinaus auf Big Data, KI, IoT und andere aufkommende digitale Anwendungen gerichtet. Es ist jedoch auch bekannt, dass APIs nicht nur in der Anzahl, sondern auch im Risiko zunehmen. Nachdem andere große Telekommunikationsanbieter 2022 und 2023 unter den Auswirkungen von API-Angriffen gelitten hatten, arbeitete das Unternehmen mit Noname Security (jetzt ein Akamai-Unternehmen) zusammen.

Telecommunications Company

Standort

Asien

Branche

Netzwerkbetreiber

Lösung

Akamai API Security

Akamai

Notwendigkeit der Sichtbarkeit aller APIs und ihrer Risiken

Sicherheitsabteilungen zahlreicher Unternehmen stehen häufig vor dem Problem, dass sie nur unzureichende Einblicke in APIs und die damit verbundenen Risiken haben. Laut unserer Untersuchung wissen nur 4 von 10 Unternehmen mit vollständigen API-Beständen, welche ihrer APIs sensible Daten zurückgeben. Durch die Verwendung des Discovery-Moduls unserer API-Sicherheitslösung stellten wir fest, dass unser Telekommunikationskunde vor einer ähnlichen Herausforderung stand.

Vor der Zusammenarbeit mit Akamai bestanden die API-Sicherheitskontrollen des Kunden hauptsächlich aus einer veralteten API-Verwaltungsplattform und einer Web Application Firewall (WAF). Aus der Perspektive der Anwendungssicherheit und der API-Bereitstellung war diese Vorgehensweise sinnvoll. Allerdings bot keine der beiden Lösungen das hohe Maß an Sicherheitskontrollen und Beobachtbarkeit, das erforderlich ist, um APIs umfassend vor den Angriffsmethoden von heute zu schützen. Ein wichtiger Grund: Nicht alle APIs werden über einen Proxy wie eine WAF oder ein API-Gateway geleitet, und diese nicht verwalteten APIs sind attraktive Ziele für böswillige Akteure.

Aber selbst mit einer genauen Prüfung seines API-Bestands benötigte das Unternehmen noch Möglichkeiten, APIs während ihres normalen Betriebs zu sichern, während sie Anfragen bearbeiten und verwalten. Es wäre schlichtweg nicht machbar, wenn das Sicherheitsteam eines Unternehmens bösartiges Verhalten in seiner Umgebung manuell identifizieren müsste.

Es gibt Hunderte, wenn nicht Tausende von API-Endpunkten, die in Echtzeit geschützt werden müssen. Häufig verwendete AppSec-Lösungen können in der Regel nicht mit jedem API-Aufruf in der Umgebung eines Kunden Schritt halten. Dies kann dazu führen, dass die IT-Umgebung eines Unternehmens ohne die richtigen API-Laufzeitschutzfunktionen anfällig für Cyberangriffe ist.

Lösungen für die Sichtbarkeit aller APIs und den Schutz vor API-Bedrohungen

Die erste Phase des Projekts umfasste einen Pilotversuch, um die internen APIs des Unternehmens zu lokalisieren, Konfigurationen zu bewerten und die Datentypen zu verstehen, die die APIs durchlaufen. Der Kunde war sofort beeindruckt von der Geschwindigkeit, mit der die Untersuchung durchgeführt wurde, von den genauen Bestandsergebnissen und von den sensiblen Daten, die das Tool aufgedeckt hat.

Aufgrund der positiven Ergebnisse des Pilotprojekts erweiterte der Kunde den Abdeckungsbereich der Noname API Security Platform (jetzt Teil von Akamai API Security) auf seinen gesamten internen und externen API-Bestand. Im Rahmen dieses Tests wurden auch weitere versteckte Produktions-APIs aufgedeckt und die unmittelbarsten Bedrohungen für die Umwelt ermittelt.

Wir stellten fest, dass der Kunde einen stärkeren Schutz gegen schwerwiegende Sicherheitslücken benötigte, um seine APIs vor zukünftigen Angriffen zu schützen. Mit Akamai API Security kann der Kunde nun verdächtige Verhaltensanomalien aufdecken und Protokolle zur Reaktion auf Vorfälle auslösen – in Echtzeit. So kann ein Unternehmen vermeiden, dass es sich bei der Information über seinen Korrekturprozess auf verspätete Berichte und Zugriffsprotokolle verlassen muss. Sobald verdächtige Verhaltensweisen mit Akamai API Security erkannt werden, werden sie an das API-Gateway, das SIEM-System und andere Informationssicherheits-Engines des Kunden gemeldet, um das gesamte Sicherheitsteam zu informieren. Der Kunde kann wählen, ob seine Mitarbeiter das Problem manuell, halbautomatisch oder vollautomatisch beheben sollen, je nach Anwendungsfall und Schwere der Sicherheitslücke.

 | Veröffentlicht 09/24