Pressemitteilung

API Protection Report: Suchanfragen für Schatten-APIs steigen um 900 Prozent

Cequence Security identifiziert mangelnde API-Sichtbarkeit als großes Sicherheitsrisiko für Unternehmen

München, 17. Mai 2023 – APIs (Application Programming Interface) waren 2022 eines der führenden Angriffsziele. So sind Suchanfragen für Schatten-APIs im Vergleich zur ersten Jahreshälfte 2022 um 900 Prozent auf rund 45 Milliarden Anfragen gestiegen. Das ist eines der zentralen Ergebnisse des „API Protection Report“, den Cequence Security nun vorgestellt hat. Dafür hat der führende Anbieter von Unified-API-Protection-Lösungen etwa eine Billion API-Transaktionen im zweiten Halbjahr 2022 branchenübergreifend analysiert, die auf Consumer-Facing, Business-to-Business (B2B) und Machine-to-Machine (M2M) APIs abzielen.

„Schatten-APIs, die außerhalb eines definierten Prozesses veröffentlicht wurden, haben genauso wie gesicherte Schnittstellen Zugriff auf sensible Informationen. Im schlimmsten Fall können Angreifer geschäftskritische Daten abgreifen und hohen Schaden verursachen“, sagt Mario van Riesen, Regional Sales Director DACH & CEE bei Cequence Security.

550 Prozent mehr Taktiken: Angreifer nutzen Urlaubszeit aus
Cyberkriminelle bevorzugen für ihre Angriffstaktiken die Ferien- und Urlaubszeit. Laut API Protection Report stieg die Anzahl der Taktiken, Techniken und Verfahren, die die Angreifer verwenden, ab Juni 2022 bis zum Jahresende um 550 Prozent von 2.000 auf 11.000 Stück an. Dabei kombinieren Angreifer zunehmend API- und Web-Anwendungssicherheitstaktiken. Bei API-Sicherheitstaktiken verzeichnete Cequence Security einen Anstieg von 220 Prozent gegen Ende des Jahres.

„In den letzten Monaten waren zahlreiche Organisationen von API-Angriffen betroffen. Dabei werden die Methoden der Angreifer immer kreativer. Traditionelle Schutztechniken reichen häufig nicht mehr aus“, sagt Ameya Talwalkar, CEO und Gründer von Cequence Security. Und weiter: „Die Angriffsautomatisierung gegen APIs nimmt weiter zu. Für CISOs gilt es, die API-Schutzmaßnahmen zu verstärken, um Angriffe in Echtzeit abzuwehren.“

Ausgefeilte Bedrohungsmethoden bei Telekommunikations-APIs
Insgesamt zeigt die Analyse, dass sich das API-Bedrohungsumfeld dynamisch entwickelt. Die Angriffsflächen und -methoden sind breit gefächert. So gab es insbesondere bei Telekommunikations-APIs eine Vielzahl an neuen, ausgefeilten Bedrohungsmethoden. Für Organisationen gilt es, wachsam zu sein, um ihre APIs und Web-Anwendungen vor automatisierten Bedrohungen (Bots) und der Ausnutzung von Schwachstellen zu schützen.

Neue API-Bedrohungskategorie in OWASP API Security Top 10
Cequence Security befürwortet es daher, dass das OWASP (Open Worldwide Application Security Project) seine API Security Top 10 um die OWASP API-Bedrohungskategorie API8 (Mangelnder Schutz vor automatisierten Bedrohungen) erweitert hat und damit native Bot-Abwehrfunktionen in ein robustes API-Sicherheitsprogramm einbezogen hat.

Mit der Unified-API-Protection-Plattform bietet Cequence Security eine umfassende End-to-End-Lösung für den gesamten API-Protection-Lebenszyklus – vom Aufdecken über das Monitoren bis hin zum Schützen aller im Unternehmen vorhandenen Schnittstellen.

Der vollständige Report ist als Download verfügbar: zum „API Protection Report“

Mehr Informationen auf www.cequence.ai

Pressekontakt:

Cequence Security
Mario van Riesen
Regional Sales Director DACH & CEE
Tel.: +49 151 7219 3673
Mail: mario@cequence.ai
Web: www.cequence.ai

VOCATO public relations GmbH
Birgit Brabeck /
Friederike Wagner
Tel.: +49 2234 60198 - 18 / - 16
Mail: bbrabeck@vocato.com / fwagner@vocato.com
Web: www.vocato.com

Über Cequence Security
Cequence Security bietet innovative Anwendungssicherheitslösungen für moderne hypervernetzte Unternehmen an. Das US-amerikanische Unternehmen mit Hauptsitz in Sunnyvale, Kalifornien, hat die Unified-API-Protection-Plattform entwickelt, die API-Erkennung, Inventarisierung, Compliance und dynamisches Testen mit Echtzeit-Erkennung von Bedrohungen gegen sich ständig weiterentwickelnde Online-Angriffe in einer Lösung vereint. Hyperverbundene Unternehmen schützen damit ihre web-, mobil- und API-basierten Anwendungen vor Betrug, Geschäftsmissbrauch und Datenverlust. Gegründet 2014, sichert Cequence Security heute mehr als sechs Milliarden API-Transaktionen pro Tag und schützt mehr als zwei Milliarden Benutzerkonten der Fortune-500-Kunden. Weitere Informationen auf www.cequence.ai