Wichtige Erkenntnisse aus dem Bericht

KI-basierte APIs sind unsicherer als ihre Gegenstücke.

Der Großteil der KI-gestützten APIs ist extern zugänglich und viele von ihnen verfügen über nur unzureichende Authentifizierungsmechanismen. Diese Schwachstelle wird durch die wachsende Anzahl KI-gestützter Angriffe noch vergrößert.

KI fördert den technischen Fortschritt von Cyberkriminellen.

Dazu gehören Verbesserungen wie KI-basierte Malware, Schwachstellenscans, Angriffe auf KI-integrierte Systeme oder ausgeklügelte Web-Scraper.

32 %

Prozentuale Zunahme von Zwischenfällen in Bezug auf die OWASP API Security Top 10

API-Sicherheitsvorfälle nehmen zu, wobei die OWASP (Open Worldwide Application Security Project) API Security Top 10 darauf hindeuten, dass Authentifizierungs- und Autorisierungsfehler, die vertrauliche Daten und Funktionen offenlegen, die größten Probleme darstellen.

30 %

Zunahme der Sicherheitswarnungen im Zusammenhang mit dem MITRE-Sicherheitsframework

Angreifer nutzen fortschrittliche Techniken, einschließlich Automatisierung und KI, um APIs auszunutzen. Das MITRE-Framework kann Verteidiger dabei unterstützen, diese Angriffe schneller und genauer zu erkennen.

33 %

Prozentuale Zunahme globaler Webangriffe im Jahresvergleich

Die Zunahme der Angriffe steht in direktem Zusammenhang mit der schnellen Einführung von Cloud-Services, Microservices und KI-Anwendungen, die die Angriffsflächen erweitern und neue Sicherheitsherausforderungen mit sich bringen.

Über 230 Milliarden

Anzahl der Webangriffe, die Handelsorganisationen getroffen haben

Damit ist der Handel die am stärksten betroffenen Branche. Er verzeichnete fast dreimal so viele Angriffe wie die Hightech-Branche (die am zweithäufigsten angegriffene Branche).