# Wichtige Erkenntnisse aus dem Bericht

Der EMEA Snapshot ist eine Ergänzung zu unserem umfassenderen SOTI-Bericht zur Anwendungssicherheit Digitale Festungen unter Beschuss: Bedrohungen für moderne Anwendungsarchitekturen (nur in englischer Sprache verfügbar). In diesem Bericht finden Sie eine detaillierte Beschreibung dazu, wie Angreifer die immer größeren Angriffsflächen ausnutzen, Empfehlungen, um Ihr Unternehmen zu schützen, sowie eine ausführliche Erklärung unserer Forschungsmethoden.

## Übersicht

Die vergangenen zwei Jahrzehnte waren von einem rasanten Anstieg sowohl der Quantität als auch der Funktionsvielfalt von Webanwendungen gekennzeichnet. Diese Entwicklung führt zur Optimierung von Geschäftsprozessen sowie der Verbesserung von Kundenerlebnissen und steigert das Wachstum durch Funktionen wie Echtzeitkommunikation, Datenanalyse und Prozessautomatisierung. APIs, die Grundlage der Kommunikation zwischen Anwendungen, haben sich ebenfalls stark weiterentwickelt und werden künftig eine noch größere Rolle spielen.

Anwendungen sind nahezu an jedem Aspekt von Unternehmen beteiligt. Sie erleichtern Billionen von Verbindungen, machen diese jedoch auch anfälliger für Angriffe. In diesem EMEA Snapshot, der den Zeitraum von Januar 2023 bis Juni 2024 betrachtet, bieten wir einen ganzheitlichen Überblick über die Bedrohungen, von denen Anwendungen betroffen sind – einschließlich Webangriffe, DDoS-Angriffe (Distributed Denial of Service) und Bedrohungen für kritische Workloads – wobei der Schwerpunkt darauf liegt, was diese Bedrohungen für Sie bedeuten.

Die Anzahl der DDoS-Angriffe auf Layer 3 und Layer 4 stieg in der EMEA-Region (Europa, Naher Osten und Afrika) kontinuierlich an und übertraf die Angriffszahlen in Nordamerika in fünf der letzten sieben Monate. Der Finanzdienstleistungssektor war dabei am stärksten betroffen.

Die monatlichen Aktivitäten für Angriffe auf Webanwendungen und APIs in der EMEA-Region stiegen zwischen Q1 2023 und Q1 2024 um 21 % an, wobei Angriffe auf APIs im Durchschnitt 40 % der monatlichen Webangriffe ausmachten.

Der Handel war die von Webangriffen am stärksten betroffene Branche in EMEA. Das zeigte sich in einem hohen Prozentsatz von API-Angriffen. Der Handel war außerdem die Branche, in der die meisten DDoS-Angriffe auf Layer 7 stattfanden.

Ransomware und andere Angriffe auf Anwendungen sowie auf interne Workloads zwischen Anwendungen werden zunehmend zum Problem. Unternehmen setzen auf softwarebasierte Mikrosegmentierung, um Transparenz und detaillierte Kontrollen zu gewährleisten, die zum Schutz dieser wachsenden Angriffsfläche erforderlich sind.