SOTI

B10 AUSGABE 04

10 YEARS
OF SECURITY INSIGHT

Bedrohungen für moderne Anwendungsarchitekturen

EMEA Snapshot

Akamai

„State of the Internet“-Sicherheitsbericht

Inhaltsverzeichnis

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.

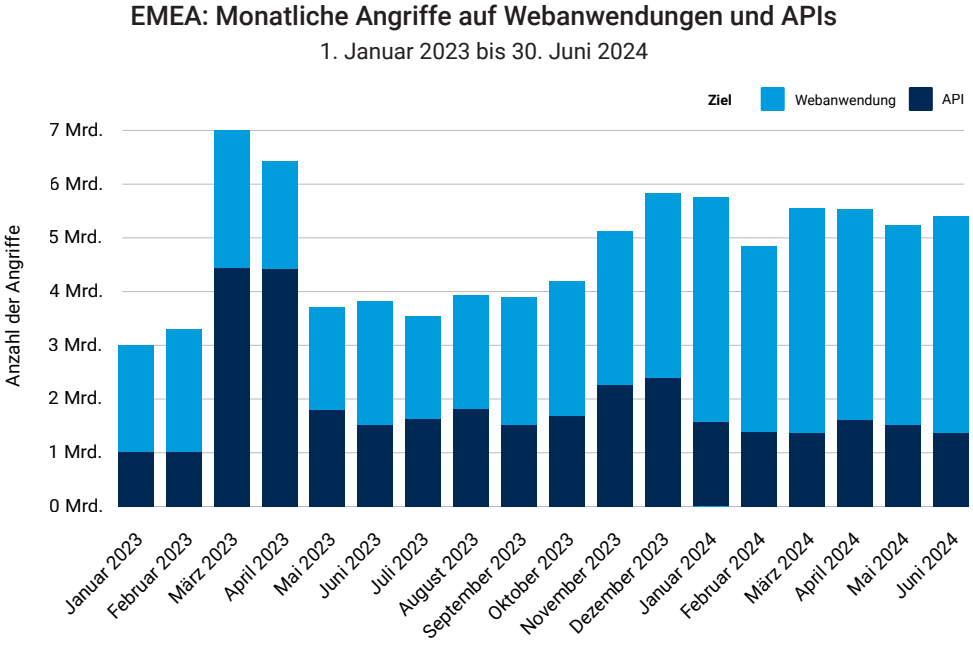
Ransomware und andere Angriffe auf Anwendungen sowie auf interne Workloads zwischen Anwendungen werden zunehmend zum Problem. Unternehmen setzen auf softwarebasierte Mikrosegmentierung, um Transparenz und detaillierte Kontrollen zu gewährleisten, die zum Schutz dieser wachsenden Angriffsfläche erforderlich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

Webanwendungen und APIs: Quellen für umfangreiche Sicherheitsrisiken

Angriffe auf Webanwendungen und APIs werden immer häufiger, da Unternehmen Anwendungen bereitstellen, um das Kundenerlebnis zu verbessern und die betriebliche Effizienz zu optimieren. Cyberkriminelle nutzen die Schwachstellen in dieser Angriffsfläche aus (z. B. Webanwendungen mit fehlerhaftem Programmcode, Designfehlern und mehrere Jahre alten Schwachstellen). Darüber hinaus bietet die rasche Expansion der API-Wirtschaft Cyberkriminellen weitere Möglichkeiten, um Schwachstellen auszunutzen und Geschäftslogik zu missbrauchen.

Angriffstrends in Zahlen

In unserem ersten SOTI-Bericht für 2024 haben wir die API-Angriffstrends im Jahr 2023 im Kontext der gesamten Angriffe auf Webanwendungen untersucht. Im Rückblick auf die letzten 18 Monate, von Januar 2023 bis Juni 2024, haben die Forscher von Akamai festgestellt, dass die monatlichen Angriffe auf Webanwendungen und APIs im EMEA-Raum vom Q1 2023 zum Q1 2024 um 21 % gestiegen sind und bis zum 2. Quartal 2024 weiterhin erhöht blieben. API-Angriffe trugen zu diesem anhaltenden Aktivitätsgrad bei und machten durchschnittlich 40 % der monatlichen Webangriffe in diesem Zeitraum aus (EMEA Abbildung 1).



EMEA Abb. 1: Die monatlichen Angriffe auf Webanwendungen und APIs sind im Jahr 2024 weiterhin erhöht (HINWEIS: Der Anstieg bei API-Angriffen ist mit dem Handelssektor in Spanien assoziiert, einem Land mit einer bereits hohen API-Angriffsdichte.)

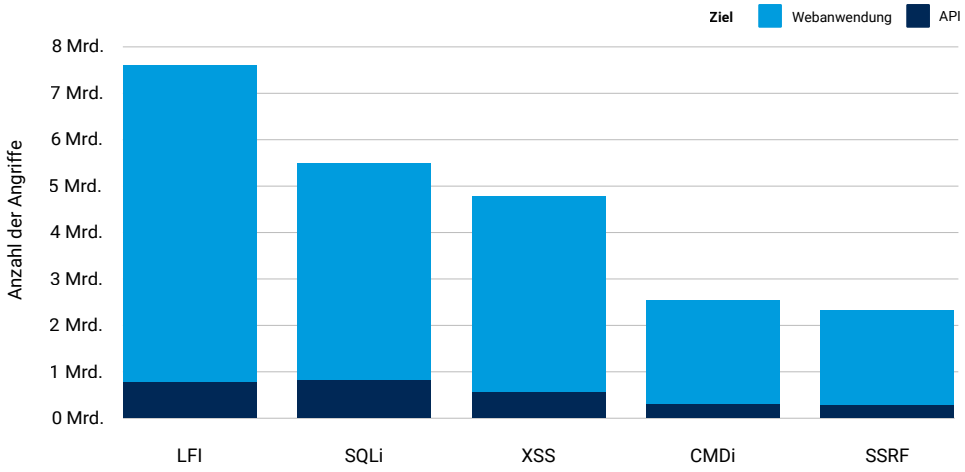
Innerhalb der EMEA-Region hatten das Vereinigte Königreich (20,5 Mrd.), die Niederlande (15,6 Mrd.) und Spanien (12,7 Mrd.) die meisten Angriffe auf Webanwendungen und APIs zu verzeichnen. Deutschland (8,7 Mrd.), Österreich (7,4 Mrd.), Frankreich (4,8 Mrd.), Israel (3,0 Mrd.), Italien (2,7 Mrd.), die Schweiz (2,5 Mrd.) und Belgien (2,3 Mrd.) vervollständigen die Top 10.

Akamai hat zudem mehrere Angriffsvektoren für Webangriffe im Blick. In diesem Bericht konzentrieren wir uns auf die fünf wichtigsten klassischen vektorbasierten Angriffsmethoden.

Im Einklang mit vorherigen Berichten blieb Local File Inclusion (LFI) ein bevorzugter Angriffsvektor, aber auch andere Vektoren wie Structured Query Language Injection (SQLi) und Cross-Site Scripting (XSS) geben Anlass zur Sorge (EMEA Abbildung 2).

EMEA: Die fünf wichtigsten herkömmlichen Webangriffsvektoren

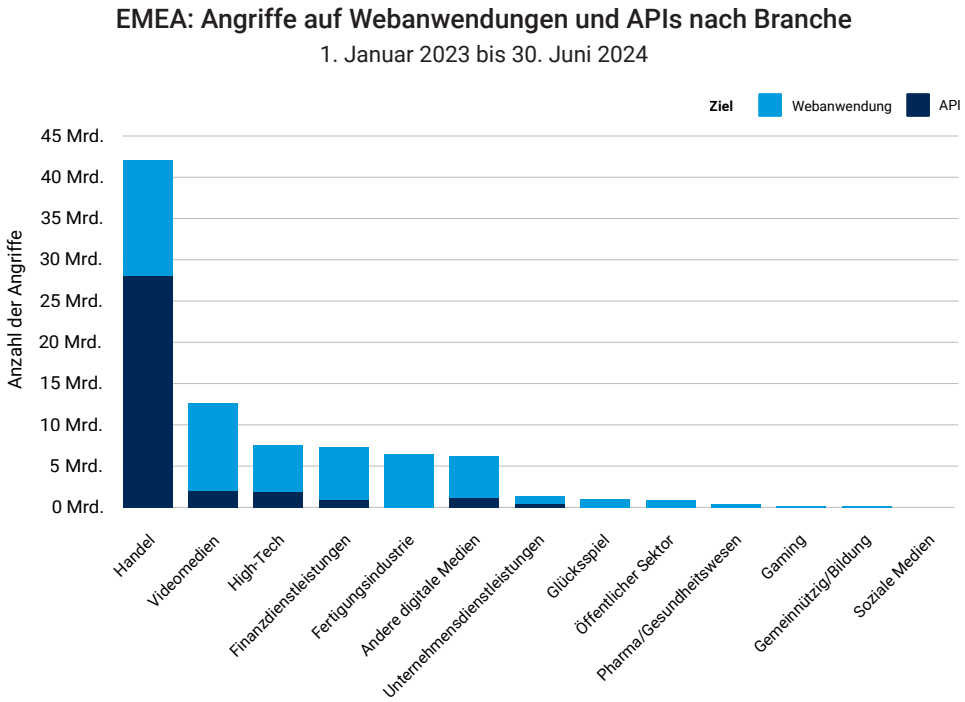
1. Januar 2023 bis 30. Juni 2024



EMEA Abb. 2: LFI, SQLi und XSS bedingen eine Zunahme der Angriffe auf APIs und Webanwendungen.

Angreifer nutzen regelmäßig klassische Techniken wie LFI und SQLi, um auf die Daten ihrer Ziele zuzugreifen. LFI ermöglicht Angreifern, sich in ihre Ziele einzuschleusen und Remotecode auszuführen, was ein zusätzliches Sicherheitsrisiko darstellt.

Als Fortsetzung des Trends, den wir in vorherigen Berichten beschrieben haben, waren im EMEA-Raum die Bereiche Handel und Videomedien am stärksten von Angriffen auf Webanwendungen und APIs betroffen. Wie wir in unserem SOTI-Bericht zur API-Sicherheit besprochen haben, verzeichnete der Handel im Vergleich zu anderen Sektoren in der Region weiterhin den höchsten Prozentsatz an API-Angriffen (EMEA Abbildung 3).



EMEA Abb. 3: Aufgrund des besonders großen Anteils an API-Angriffen war der Handelssektor am stärksten von Webangriffen betroffen, gefolgt von Videomedien, Hightech und Finanzdienstleistungen.

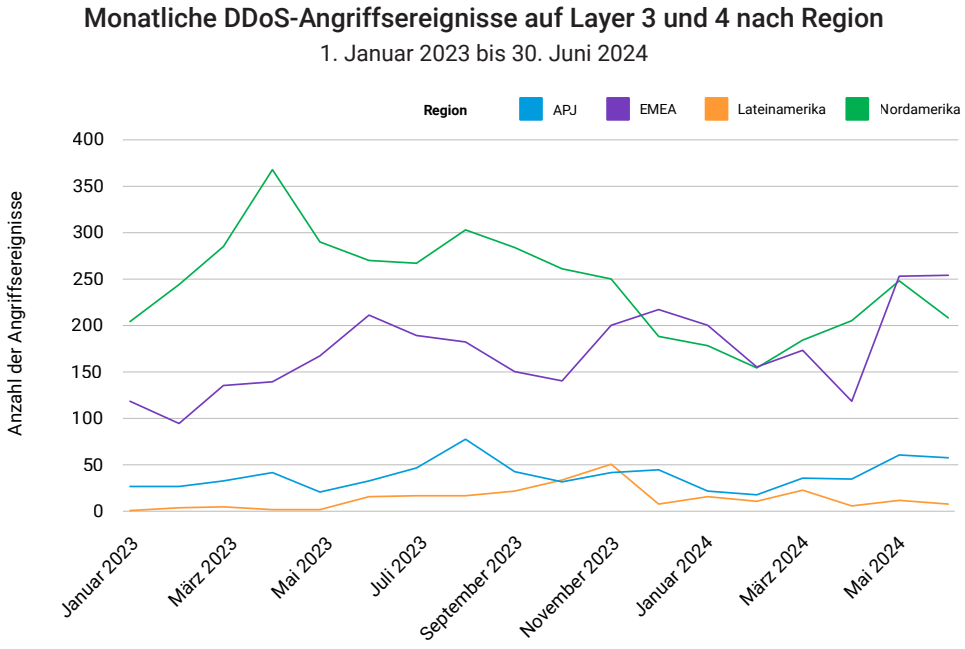
DDoS-Angriffe bedrohen die Verfügbarkeit von Anwendungen

Mit wachsender Angriffsfläche nehmen auch die DDoS-Angriffstypen zu, von denen Anwendungen betroffen sind. Wie im globalen SOTI-Bericht ausführlicher erläutert, kursieren DDoS-Angriffe auf klassische Infrastrukturen (Layer 3 und Layer 4) bereits am längsten und zielen darauf ab, die Kapazität von Netzwerken oder Anwendungsservern zu überlasten. DDoS-Angriffe auf Anwendungsebene (Layer 7) nutzen Schwachstellen und Lücken und/oder Fehler in der Geschäftslogik auf Anwendungsebene aus. Sie können selbst mit relativ geringen Mengen an schädlichem Traffic erheblichen Schaden verursachen. Unabhängig von der Angriffsmethode führen erfolgreiche DDoS-Angriffe stets zu Anwendungsausfällen.

Das Spektrum der DDoS-Angriffstypen und -trends in der Region wird in unserem kürzlich publizierten SOTI für den EMEA-Raum 2024 eingehend untersucht. Hier zeigen wir aktualisierte Daten, die einen anhaltenden Anstieg von DDoS-Bedrohungen auf Layer 3, 4 und 7 für Anwendungsinfrastrukturen sowie für die Anwendungen selbst beschreiben.

DDoS-Angriffe auf die Infrastruktur

Forscher von Akamai stellten fest, dass während des 18-monatigen Berichtszeitraums von Januar 2023 bis Juni 2024 die Anzahl der DDoS-Angriffsereignisse auf Layer 3 und 4 im EMEA-Raum stetig gestiegen ist und die Anzahl der monatlichen DDoS-Angriffsereignisse in Nordamerika in fünf der letzten sieben Monate überstieg (EMEA Abbildung 4).



EMEA Abb. 4: Die Zahl der monatlichen DDoS-Angriffe auf Layer 3 und 4 in EMEA war in fünf der letzten sieben Monate höher als in Nordamerika

Innerhalb des EMEA-Raums waren Saudi-Arabien (957) und das Vereinigte Königreich (576) gefolgt von der Schweiz (240), der Türkei (205), Italien (203), Deutschland (189) und Polen (115) am stärksten von DDoS-Angriffen auf Layer 3 und 4 betroffen.

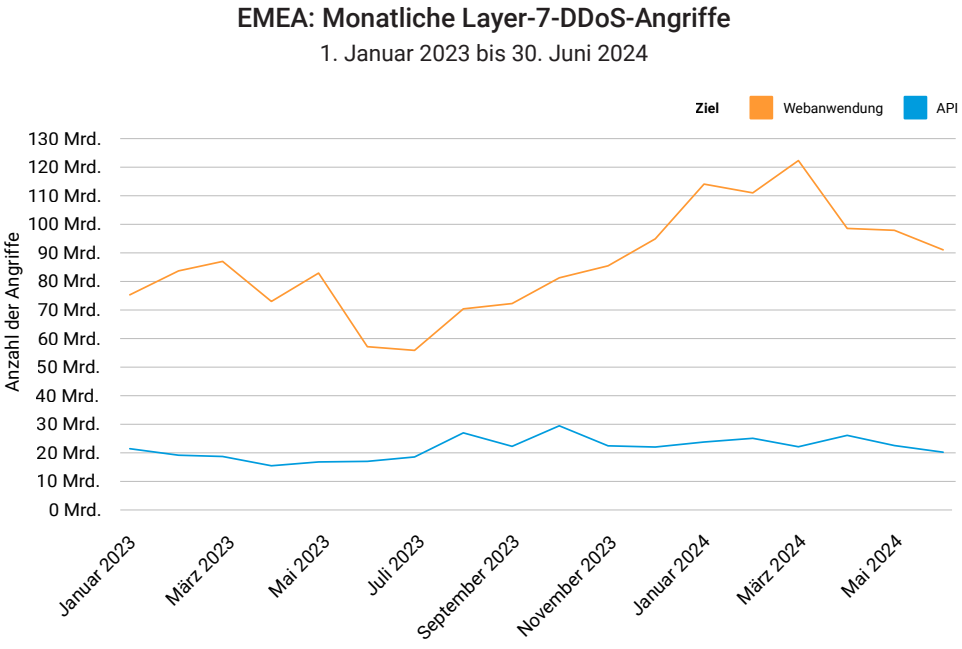
Wie in unserem SOTI-Bericht für den EMEA-Raum erwähnt, ist DDoS ein beliebtes Werkzeug für politisch motivierte Hacktivisten und staatlich finanzierte Angreifer. Die Konflikte zwischen Russland und der Ukraine sowie zwischen Israel und der Hamas haben zu einem verstärkten Aufkommen von Angriffen geführt.

Aus Branchensicht erlebten Finanzdienstleister (1.523) und die Fertigungsindustrie (890) die höchste Anzahl von DDoS-Angriffen auf Layer 3 und 4, gefolgt von Gaming (189), Handel (151), Glücksspiel (105) und Hightech (95).

DDoS-Angriffe auf Anwendungsebene

Zusätzlich zu den DDoS-Angriffen auf Layer 3 und 4 war die Region auch von DDoS-Angriffen auf Anwendungsebene (Layer 7) betroffen. Unsere Forscher berichten für den 18-monatigen Zeitraum von Januar 2023 bis Juni 2024, dass EMEA die am drittstärksten von DDoS-Angriffen auf Layer 7 betroffene Region war, mit 1,9 Billionen Anfragen im Vergleich zu 8,7 Billionen in Nordamerika und 5,1 Billionen im APJ-Raum.

Trotz ihrer geringeren Häufigkeit im Vergleich zu anderen Regionen, sollte der Anstieg der Layer-7-DDoS-Angriffe in EMEA beachtet werden. Nach einem Rückgang im Mai 2023 auf 74 Milliarden stiegen die monatlichen Layer-7-DDoS-Angriffe deutlich an und verdoppelten sich bis März 2024 beinahe, bevor das 2. Quartal 2024 mit einem monatlichen Durchschnitt von 119 Milliarden Angriffen auf Webanwendungen und APIs endete (EMEA Abbildung 5).



EMEA Abb. 5: Die Zahl der Layer-7-DDoS-Angriffe nahm seit Juni 2023 erheblich zu und belief sich zum Ende des 2. Quartals 2024 auf durchschnittlich 119 Milliarden pro Monat.

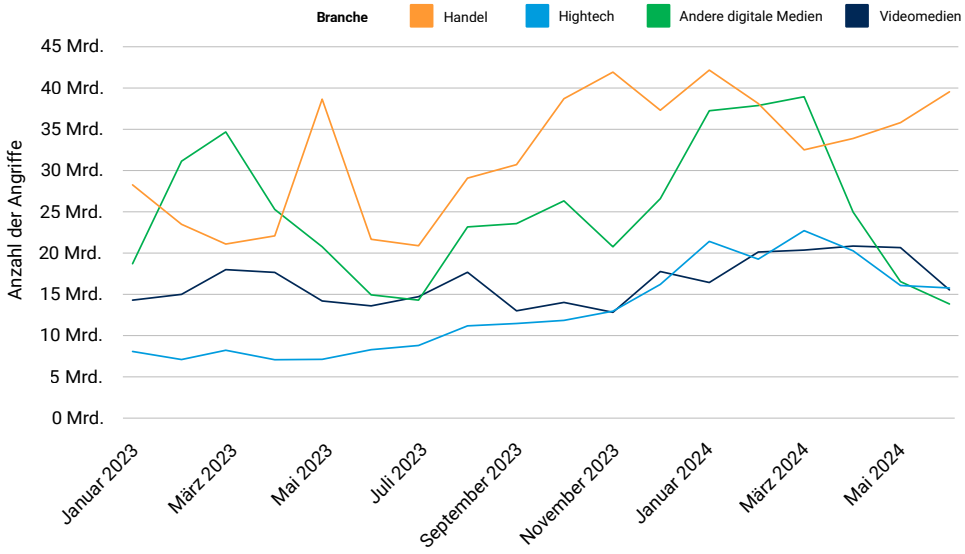
Die Zahl der DDoS-Angriffe auf APIs blieb relativ stabil und machte im gesamten Zeitraum 25 % dieser Angriffe aus. Neben dem Schutz vor den Angriffsvektoren, die zuvor in Bezug auf Webanwendungen und API-Angriffe diskutiert wurden (siehe EMEA Abbildung 2), ist der Schutz von APIs vor DDoS-Angriffen zwingend erforderlich, insbesondere da die Verwendung von APIs weiter durch Richtlinien und Vorschriften vorangetrieben wird.

Innerhalb des EMEA-Raums waren Deutschland (461 Mrd.) und das Vereinigte Königreich (366 Mrd.) die Länder mit der höchsten Anzahl von DDoS-Angriffen auf Layer 7, gefolgt von Schweden (167 Mrd.), Israel (151 Mrd.), Italien (125 Mrd.), Malta (113 Mrd.), der Schweiz (112 Mrd.), Frankreich (90 Mrd.), den Niederlanden (79 Mrd.) und Spanien (77 Mrd.).

Die Betrachtung der Branchen zeigt, dass der Handel am stärksten von Layer-7-DDoS-Angriffen betroffen war, sowohl zu Beginn als auch am Ende des Zeitraums, gefolgt von anderen digitalen Medien, Videomedien und Hightech (siehe EMEA Abbildung 6).

EMEA: Monatliche DDoS-Angriffe auf Layer 7 nach Branche

1. Januar 2023 bis 30. Juni 2024



EMEA Abb. 6: Der Handel war am stärksten von DDoS-Angriffen auf Layer 7 betroffen.

Angreifer zielen auf Anwendungsworkloads ab

Zero Trust wird in der Regel im Kontext der Netzwerksicherheit diskutiert. Webanwendungen und die internen Workloads zwischen ihnen können jedoch auch Bedrohungen wie Ransomware ausgesetzt sein, die nach einem beliebigen Einstiegspunkt und Pfad suchen, um ihre Ziele zu erreichen.

Wie im globalen Bericht ausführlich erläutert, muss jede einzelne Workload nahtlos ausgeführt werden, damit Anwendungen funktionieren – ob in der Cloud, vor Ort oder in hybriden Umgebungen. Workloads durchlaufen mehrere Sicherheitsterritorien, während sie sich durch das Netzwerk bewegen, wobei jedes Territorium einen potenziellen Einstiegspunkt für Eindringlinge bietet. Der Schutz dieser ausgedehnten Angriffsfläche ist entscheidend für die Stärkung der allgemeinen Sicherheitslage, erschwert jedoch die ohnehin schwierigen Aufgaben der Sicherheitsteams.

Die Implementierung eines Zero-Trust-Frameworks auf Basis eines herkömmlichen hardwarebasierten Ansatzes ist ein ressourcen- und zeitintensives Unterfangen, für das Ausfallzeiten erforderlich sind. Darüber hinaus ist für eine echte Zero-Trust-Implementierung Mikrosegmentierung erforderlich, die vor Ransomware oder Angriffen auf die Workloads selbst schützen kann.

Softwarebasierte Mikrosegmentierung lässt sich schnell und einfach implementieren und verwenden. Sie dient sowohl zur effektiven Reaktion auf Vorfälle als auch zur Isolierung kritischer Systeme und unterstützt so die Einhaltung gesetzlicher Vorschriften. Zudem ermöglicht sie eine tiefgreifende Visualisierung des Netzwerks und detaillierte Governance-Kontrollen. Aufgrund dieser Vorteile greifen Unternehmen zunehmend auf das Konzept zurück, um gefährdete Workloads oder Container in dynamischen Rechenzentren sowie in Cloud- und Hybrid-Cloud-Umgebungen zu erkennen und abzusichern.

Praxisnahe Einblicke zum Schutz von Anwendungsworkloads

In diesem Abschnitt stellen wir zwei Fallstudien aus der EMEA-Region vor, die beispielhaft zeigen, wie Unternehmen kritische Workloads sichern und Zero Trust umsetzen.

EMEA-Fallstudie 1: Um kritische Systeme und sensible Daten im Handel und Zahlungsverkehr zu schützen, überprüft der Chief Information Security Officer (CISO) einer führenden Investmentbank regelmäßig die Sicherheit der Technologieinfrastruktur, um diese in allen Bereichen zu stärken. Ein großer Schwerpunkt liegt auf der Bekämpfung von Ransomware-Angriffen sowie auf der Skalierbarkeit und Abdeckung verschiedener Betriebssysteme und Cloudumgebungen. Darüber hinaus suchte der CISO nach einer Möglichkeit zur Reduzierung der Angriffsfläche, ohne die mit der Aktualisierung älterer Firewalls verbundenen Kosten und Verzögerungen in Kauf nehmen zu müssen. Anwendungsworkloads wurden durch die Implementierung einer softwarebasierten Mikrosegmentierung, die sichere Zonen in Rechenzentren schafft, voneinander getrennt. Wenn eine Workload angegriffen wird, kann sie isoliert werden, wodurch die Verbreitung schädlicher Software im Netzwerk verhindert wird.

EMEA-Fallstudie 2: Ein Medien- und Softwareanbieter sucht nach einem einfacheren Konzept, um sein Zero-Trust-Framework zu erweitern, um kritische Workloads und Kundendaten besser zu schützen. Um diese Verbesserung umzusetzen, war es unerlässlich, hochwertige Komponenten wie Identitätsmanagement-Systeme und Planungssysteme für Unternehmensressourcen durch präzise Segmentierungsrichtlinien voneinander zu trennen. Ziel war es, den ein- und ausgehenden Traffic zu minimieren und die Zugriffsrichtlinien für Hunderte von Unternehmensservern zu verschärfen. Gleichzeitig wollte das Unternehmen größere Veränderungen des Ökosystems vermeiden, die zu Unterbrechungen und erhöhten Sicherheitsrisiken führen könnten. Ein softwarebasierter Mikrosegmentierungsansatz mit detaillierten Einblicken in Interaktionsmuster und Benachrichtigungsfunktionen ermöglichte es dem Team, schädliche laterale Bewegungen innerhalb des gesamten Netzwerks zu verhindern.

Fazit

In diesem EMEA Snapshot haben wir einen umfassenden Überblick über die verschiedenen Methoden geboten, die Cyberkriminelle für gezielte Angriffe auf Ihre APIs nutzen. Für das Sicherheits- und Risikomanagement ist es unerlässlich, dass Unternehmen Bedrohungen ihrer Anwendungen, APIs, Infrastruktur und kritischen Workloads verstehen und sich entsprechend schützen. Aufgrund aktueller und künftiger Gesetzgebung muss zudem ein angemessener Anwendungsschutz bereitgestellt werden.

Innerhalb des EMEA-Raums gelten in der Europäischen Union die folgenden wichtigen Gesetze: die aktualisierte Richtlinie für Netzwerk- und Informationssysteme (NIS2), der Digital Operational Resilience Act, der Cyber Resilience Act, das Europäische Programm für den Schutz kritischer Infrastrukturen, der neue Payment Card Industry Data Security Standard v4.0 und die bevorstehende überarbeitete EU-Zahlungsdiensterichtlinie (PSD3).

Anwendungen sind wichtiger denn je für Unternehmen, aber auch anfälliger für Angriffe. Mit Funktionen und Best Practices zur Bewältigung der ständig wachsenden Angriffsfläche können Unternehmen ihre Anwendungen jederzeit und überall schützen, ohne dabei die Performance oder das Kundenerlebnis zu beeinträchtigen.

Weitere Informationen finden Sie im globalen SOTI-Bericht zur Anwendungssicherheit „Digitale Festungen unter Beschuss: Bedrohungen für moderne Anwendungsarchitekturen“.

Methodik

Angriffe auf Webanwendungen und Layer-7-DDoS-Angriffe

Diese Daten beschreiben Warnungen auf Anwendungsebene über Traffic, der unsere Web Application Firewall (WAF) durchläuft. Die Anwendungsangriffswarnungen werden ausgelöst, wenn wir innerhalb einer Anfrage an eine geschützte Website, Anwendung oder API eine schädliche Payload erkennen. Die Layer-7-DDoS-Warnungen werden ausgelöst, wenn wir volumetrische Anomalien bei der Anzahl der Anfragen an eine geschützte Website, Anwendung oder API erkennen. Diese Warnungen können sowohl von schädlichen als auch von gutartigen Anfragen ausgelöst werden. In der Regel sind die Anfragen selbst harmlos, aber ihre hohe Anzahl weist auf eine böswillige Absicht hin. Die Warnungen zeigen nicht an, ob ein Angriff erfolgreich war. Obwohl diese Produkte ein hohes Maß an Anpassung ermöglichen, haben wir die hier dargestellten Daten auf eine Weise erfasst, bei der keine nutzerdefinierten Konfigurationen der geschützten Ressourcen berücksichtigt werden.

Die Daten stammen aus einem internen Tool zur Analyse von Sicherheitsereignissen, die in der Akamai Connected Cloud erkannt wurden, einem Netzwerk aus ca. 340.000 Servern an mehr als 4.000 Standorten in fast 1.300 Netzwerken in über 130 Ländern. Diese Daten werden in Petabyte pro Monat gemessen und von unserem Sicherheitsteam verwendet, um Angriffe zu untersuchen, schädliches Verhalten aufzudecken und zusätzliche Informationen in die Lösungen von Akamai einzuspeisen.

Diese Daten decken den Zeitraum von 18 Monaten vom 1. Januar 2023 bis zum 30. Juni 2024 ab.

Datenaktualisierung 2024

Wir freuen uns, anlässlich unseres 10-jährigen Jubiläums einige Updates unserer Datensätze ankündigen zu können! Unser Datensatz zu Angriffen auf Webanwendungen wurde aktualisiert. Die Erfassungsmethode wurde umgestaltet, gestrafft und optimiert. Umfang und Tiefe unserer Einblicke wurden erweitert. Klassifizierungen für zusätzliche Angriffsvektoren, wie z. B. SSRF, wurden hinzugefügt. Die Erkennung von Angriffen auf API-Endpunkte wurde ebenfalls zum Datensatz hinzugefügt. Wir freuen uns, Ihnen in diesem Bericht unsere neuen Verbesserungen vorstellen zu können. Im Laufe des Jahres und darüber hinaus werden wir weitere Entwicklungen mit Ihnen teilen. Gemeinsam mit Ihnen, unseren Lesern, feiern wir diesen bedeutenden Meilenstein für die SOTI-Sicherheitsberichte.

DDoS (Layer 3 und 4)

Akamai Prolexic Routed schützt Unternehmen vor DDoS-Angriffen, indem es Attacken und anderen unerwünschten oder schädlichen Traffic in der Cloud stoppt, bevor sie Anwendungen, Rechenzentren und die Cloud- und Hybrid-Internetinfrastruktur (öffentlich oder privat), einschließlich aller Ports und Protokolle, erreichen können. Experten im Security Operations Command Center (SOCC) von Akamai passen proaktive Abwehrkontrollen so an, dass Angriffe sofort erkannt und gestoppt werden. Außerdem führen sie eine Live-Analyse des verbleibenden Traffics durch, um bei Bedarf weitere Abwehrmaßnahmen einzusetzen. Diese abgewehrten Angriffe werden organisiert und in Angriffsereignisse gruppiert und alle zugehörigen Daten werden vom SOCC zur Analyse aufgezeichnet.

Diese Daten decken den Zeitraum von 18 Monaten vom 1. Januar 2023 bis zum 30. Juni 2024 ab.

Mitwirkende

Forschungsleitung

Mitch Mayne

Redaktion und Text

Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Maria Vlasak

Prüfung und Fachleute

Sven Dummer
Reuben Koh
Tony Lauro
Richard Meeus
Menacham Perlman
Sandeep Rath
Steve Winterfeld

Datenanalyse

Chelsea Tuttle

Werbematerialien

Barney Beal

Marketing und Veröffentlichung

Georgina Morales
Emily Spinks

Weitere „State of the Internet“-Sicherheitsberichte

Lesen Sie vorherige Ausgaben und informieren Sie sich über bevorstehende Veröffentlichungen der renommierten „State of the Internet“-Sicherheitsberichte von Akamai. **akamai.com/soti**

Weitere Informationen zur Bedrohungsforschung von Akamai

Halten Sie sich unter diesem Link zu neuesten Threat-Intelligence-Analysen, Sicherheitsberichten und Cybersicherheitsforschung auf dem Laufenden. **akamai.com/security-research**

Greifen Sie auf Daten aus diesem Bericht zu

Sehen Sie sich die hochauflösenden Versionen der Diagramme und Grafiken an, auf die in diesem Bericht verwiesen wird. Diese Bilder können kostenlos verwendet und referenziert werden, vorausgesetzt, Akamai wird ordnungsgemäß als Quelle genannt und das Akamai-Logo wird beibehalten. **akamai.com/sotidata**

Weitere Informationen zu Akamai-Lösungen

Weitere Informationen zu den Akamai-Lösungen zum Schutz vor Angriffen auf Anwendungen und APIs finden Sie auf unserer **Seite zu Anwendungs- und API-Sicherheit**.