State of the Internet

Der hohe Einsatz von Innovationen

Angriffstrends in der Finanzdienstleistungsbranche

In einer Zeit, die von beispielloser digitaler Transformation geprägt ist, steht die Finanzdienstleistungsbranche am Scheideweg zwischen Innovation und Risiko. Die Technologie verändert die Landschaft von Finanztransaktionen und stellt gleichzeitig eine neue Art der Bedrohung für die wirtschaftliche Stabilität dar.

Angriffe auf Finanzdienstleistungen und ihre Kunden

9 Milliarden

Anzahl der Angriffe auf Webanwendungen und APIs von Finanzdienstleistern

Nummer 1

Die Finanzdienstleistungsbranche ist mit den meisten DDoS-Angriffen am schwersten betroffen und „überholt" damit sogar die Gaming-Branche

50,6 %

Die Finanzdienstleistungsbranche verzeichnet im 2. Quartal 2023 die meisten Phishing-Angriffe

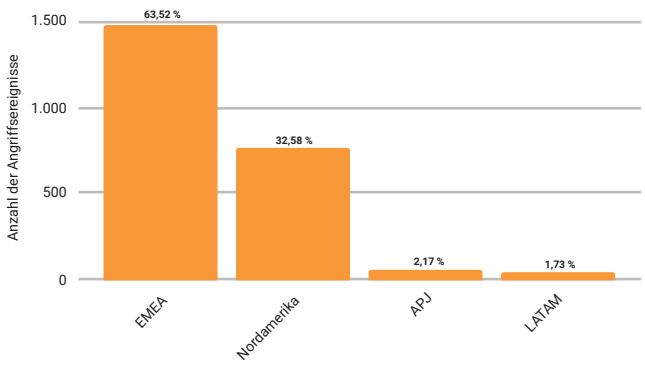
Über 1 Billion

Anzahl schädlicher Bot-Anfragen

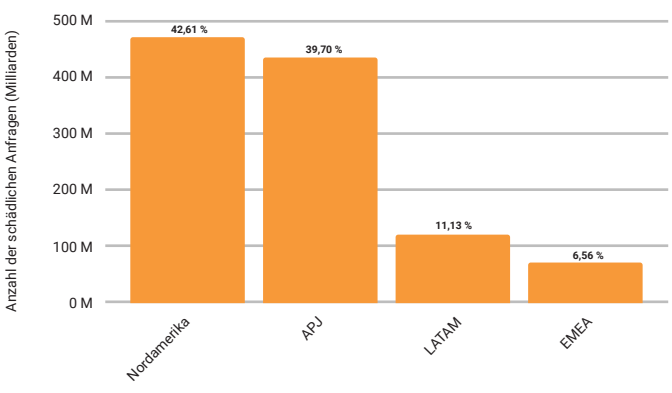
Regionale Snapshots

DDoS-Angriffsereignisse nach Regionen: Finanzdienstleistungen
1. Januar 2022 bis 30. Juni 2023

Die Anzahl der Layer-3- und Layer-4-DDoS-Angriffe in Europa, dem Nahen Osten und Afrika (EMEA) ist fast doppelt so hoch wie in Nordamerika.



Anzahl schädlicher Bot-Anfragen nach Region: Finanzdienstleistungen
1. Januar 2022 bis 30. Juni 2023



Der asiatisch-pazifische Raum und Japan (APJ) sind das zweithäufigste Ziel für schädliche Bot-Anfragen.

Potenzielle Sicherheitsrisiken

Shadow-APIs

Nicht dokumentierte und nicht nachverfolgte APIs können Überwachungsprobleme für Unternehmen darstellen, die nicht wissen, wer diese APIs auf welche Weise verwendet.

Drittanbieterskripte

Angreifer können clientseitige Schwachstellen ausnutzen oder schädlichen Code in Skripte von Drittanbietern einschleusen, die als Teil der Website geladen werden. Dadurch sind Finanzdienstleistungen dem Risiko des Web-Skimming ausgesetzt, was dazu führen kann, dass Kundendaten gestohlen oder für nicht autorisierte Transaktionen verwendet werden.

Finanzaggregatoren

Die Sicherheitslücken zwischen Finanzaggregatoren und der Art und Weise, wie Daten gesammelt werden, können Angreifern neue Möglichkeiten zur Ausnutzung eröffnen; die Folge ist Identitätsdiebstahl.

Sicherheitsempfehlungen und Best Practices

- Machen Sie sich mit Ihrer Angriffsfläche vertraut, um Strategien zur Abwehr zu entwickeln und Sicherheitskontrollen einzurichten.
- Stellen Sie API-Sicherheitstools zur Erkennung und Überwachung von nicht autorisierten APIs bereit.
- Wenden Sie die OWASP API Security Top 10 und das MITRE ATT&CK Framework an, um Schulungen und Testpläne für Ihre Red-Team- und Penetrationstestgruppen zu entwickeln.
- Nutzen Sie eine mehrschichtige Verteidigungsstrategie, die regelmäßige Sicherheitsprüfungen sowie die Implementierung erweiterter Erkennung und Abwehr umfasst.
- Nutzen Sie Lösungen wie Client-Side Protection & Compliance (ehemals Page Integrity Manager), um die Risiken von clientseitigen Angriffen zu mindern.
- Erstellen Sie ein Edge-basiertes Governance-Modell, um Transparenz im Bot-/API-Traffic zu bieten.
- Führen Sie eine Live-Übung durch, wenn Sie in den letzten drei Quartalen keinen DDoS-Angriff hatten. Validieren Sie Ihre Playbooks, und verfolgen Sie Trends hinsichtlich Größe und Geschwindigkeit, um Ihr Risiko anhand der aktuellen Möglichkeiten zu bewerten.

Weitere Informationen und Einblicke zu Angriffstrends in der Finanzdienstleistungsbranche finden Sie in unserem vollständigen Bericht.

Bericht herunterladen

 | Support | Veröffentlicht: 10/23