SOTI

10 YEARS
OF SECURITY INSIGHT

B10 AUSGABE 05

Gegen die steigende Angriffsflut

Trends in der Finanzdienstleistungsbranche

Akamai

„State of the Internet“-Sicherheitsbericht

Inhaltsverzeichnis

2	Einführung
3	*FS-ISAC-Gastkolumne*: Stärkung von Finanzdienstleistungen durch Compliance, betriebliche Resilienz und Cybersicherheit
4	Wichtige Einblicke
5	Finanzdienstleistungen bleiben das wichtigste Ziel für Layer-3- und Layer-4-DDoS-Angriffe
9	*Sicherheit im Fokus*: Intensität von DDoS-Angriffen auf Layer 3 und 4: Ereignisse im Vergleich zu Gbit/s
12	Zunehmende Layer-7-DDoS-Angriffe auf APIs
14	Ransomware und Hacktivismus in der Finanzdienstleistungsbranche
17	Auf Vertrautheit setzen: Markenmissbrauch in der Finanzdienstleistungsbranche
23	Betrügerische Finanzdienstleistungsseiten auf kritischer Risikostufe
24	Die Anatomie des Markenmissbrauchs
26	Regionale Phishing- und Imitationsangriffe im Finanzdienstleistungssektor
28	*Gastkolumne*: Weiterentwicklung der Compliance: Wie globale Cybersicherheitsvorschriften Finanzinstitute prägen
29	Mit Zero Trust zu einer starken Abwehr
31	Abwehr
33	Fazit
34	Methodik
36	Mitwirkende

Einführung

Die Finanzdienstleistungsbranche ist nicht nur ein Eckpfeiler der Weltwirtschaft, sie ist auch lebenswichtig für wirtschaftliches Wachstum und Entwicklung. Finanzdienstleistungen sind vielfältig. Es gibt zum Beispiel Geschäftsbanken, Zahlungsabwickler, Vermögensverwalter, Investmentbanken und Versicherungsorganisationen, und die Branche entwickelt sich ständig weiter.

Der technologische Fortschritt verändert die Finanzdienstleistungslandschaft und führt zu Innovationen im Bereich der Finanztechnologie (Fintech) wie digitale Banken, Robo-Berater und kryptografische Assets. Die Zahl der Fintech-Unternehmen ist weltweit sprunghaft angestiegen, wobei die Vereinigten Staaten und China führend sind. Im Januar 2024 befanden sich 8 der 10 größten Fintech-Unternehmen in diesen beiden Ländern. Dieser technologische Wandel spiegelt sich auch in der Zunahme des bargeldlosen Zahlungsverkehrs wider, der vor allem dort, wo der Zugang zu Finanzdienstleistungen eingeschränkt ist, deutlich zunehmen dürfte. Aber Innovation bringen auch Sicherheitsprobleme mit sich.

Cyberkriminelle nehmen unnachgiebig Finanzinstitute ins Visier und die Auswirkungen ihrer Angriffe gehen weit über finanzielle Verluste hinaus. Betriebsunterbrechungen, Rufschädigungen und lähmende regulatorische Strafen können das Vertrauen untergraben, die das Fundament der Finanzdienstleistungsbranche ist. Wie können Finanzinstitute effektive Abwehrmaßnahmen in einer Zeit einrichten, in der die Raffinesse von Cyberbedrohungen mit der Geschwindigkeit der digitalen Transformation Schritt hält?

Dieser „State of the Internet“-Bericht soll Finanzdienstleistern auf der ganzen Welt – Akamai-Kunden, Cybersicherheitsforschern und Branchenführern – dabei helfen, in einer zunehmend komplexen Bedrohungslandschaft zu bestehen. Als eines der Hauptziele von Cyberkriminellen muss die Finanzdienstleistungsbranche zusammenarbeiten, um ihre kritische Infrastruktur zu sichern, Unternehmen und Kunden zu schützen, die Stabilität der Finanzmärkte zu gewährleisten und wirtschaftliche Störungen zu verhindern. Die in diesem Bericht vorgestellten Forschungsergebnisse sind eine wichtige Lektüre für all jene, die den Angreifern einen Schritt voraus sein, die kritischen Assets des Sektors stärken und das anhaltende Vertrauen und die Zuverlässigkeit gewährleisten wollen, die globalen Finanzbeziehungen zugrunde liegen.

Stärkung von Finanzdienstleistungen durch Compliance, betriebliche Resilienz und Cybersicherheit

Eine der zentralen Herausforderungen, vor denen der globale Finanzsektor heute steht, ist die dringend notwendige Verbesserung von Compliance und betrieblicher Resilienz. Die gesetzlichen Rahmenbedingungen entwickeln sich weiter, und Finanzinstitute müssen sich proaktiv anpassen, um diesen neuen Anforderungen gerecht zu werden. Die Einführung des Gesetzes über die digitale betriebliche Resilienz (Digital Operational Resilience Act, DORA) unterstreicht beispielsweise die Notwendigkeit eines leistungsstarken Frameworks, das Unterbrechungen im Zusammenhang mit Informations- und Kommunikationstechnologie (IKT) standhalten kann. DORA wird voraussichtlich im Januar 2025 in Kraft treten und gibt umfassende Resilienzstrategien für Finanzunternehmen und deren IKT-Drittanbieter vor, die Unternehmen dazu zwingen, ihre Sicherheits- und Vorfallsreaktionsfähigkeiten zu verbessern.

Die aktualisierten Leitlinien der U.S. Securities and Exchange Commission erhöhen die Notwendigkeit eines ganzheitlichen Cybersicherheitskonzepts. Finanzinstitute sind nun verpflichtet, betriebliche Resilienz und Notfallwiederherstellung in ihre Strategien einzubeziehen, wobei besonderes Augenmerk auf Cyberrisiken zu legen ist. Dazu gehört ein tiefgreifendes Verständnis dafür, wie signifikante Bedrohungen und Vorfälle die Finanzstabilität und den Geschäftsbetrieb beeinflussen können. Das Verpflichtung zur unverzüglichen Offenlegung wesentlicher Cybersicherheitsvorfälle und zur detaillierten Darlegung von Risikomanagement-Strategien in Jahresberichten bedeutet einen Paradigmenwechsel bei den regulatorischen Anforderungen. Um sich in diesem regulatorischen Umfeld zurechtzufinden, müssen Finanzinstitute mit Unternehmen zusammenarbeiten, die modernste Sicherheitslösungen und Transparenz bieten. Wie diese Studie zeigt, können Finanzdienstleister mit dem Know-how von Akamai Compliance-Anforderungen besser erfüllen und auch angesichts strenger gesetzlicher Auflagen die Integrität ihrer Betriebsabläufe aufrechterhalten.

Angesichts dieser Entwicklungen müssen Finanzinstitute einen umfassenden Ansatz verfolgen, um die Komplexität der Compliance und der operativen Resilienz zu bewältigen. Dazu gehört die Ermittlung und Priorisierung wesentlicher Risiken, die sich erheblich auf den Entscheidungsprozess von Anlegern auswirken könnten. Finanzinstitute müssen diese wesentlichen Risiken in ihr Risikomanagement-Framework einbeziehen und dafür sorgen, dass solide Pläne zur Vorfallsreaktion vorhanden sind. Der Weg zu effektiver betrieblicher Resilienz wird durch die Einführung einer mehrschichtigen, tiefgreifenden Verteidigungsstrategie geebnet. Dazu gehören die Reduzierung der Angriffsfläche durch Netzwerksegmentierung und Mikrosegmentierung, die Verschlüsselung gespeicherter Daten, die Härtung von Servern und die Verwendung von Web Application Firewalls in Verbindung mit fortschrittlichen Bedrohungserkennungssystemen. Auch kontinuierliche Überwachung und regelmäßige Sicherheitsbewertungen sind entscheidend, um Risiken schnell zu erkennen und zu mindern.

Aktivitäten zur Vorfallsreaktionsplanung, die auf aktuellen Bedrohungsinformationen und -forschungen wie den SOTI-Berichten (State of the Internet) von Akamai basieren, sind für Finanzinstitute ebenfalls von entscheidender Bedeutung. Diese Maßnahmen tragen dazu bei, plausible Szenarien zu entwickeln, und gewährleisten, dass sich Institutionen an neu entwickelte Tools, Techniken und Verfahren anpassen können. Dieser proaktive Ansatz ist entscheidend, um die betriebliche Resilienz zu gewährleisten und in einer zunehmend volatilen Bedrohungslandschaft das Vertrauen der Kunden aufrechtzuerhalten. Im Zuge der Weiterentwicklung der Finanzdienstleistungsbranche wird die Schnittstelle zwischen Compliance, betrieblicher Resilienz und Cybersicherheit weiterhin die Zukunft der Branche prägen. Durch die Einführung fortschrittlicher Sicherheitsmaßnahmen und die Verbesserung der Transparenz können Finanzinstitute die Komplexität regulatorischer Vorschriften bewältigen und ihren Betrieb schützen, um das Vertrauen zu bewahren, das für ihr Geschäft unerlässlich ist.

Teresa Walsh
Global Head of Intelligence, FS-ISAC

Wichtige Einblicke

34 %

Prozentsatz der DDoS-Angriffsereignisse auf Layer 3 und 4 im Finanzdienstleistungssektor

Finanzdienstleistungen sind nach wie vor die Branche, die am häufigsten von DDoS-Angriffen (Distributed Denial-of-Service) auf Layer 3 und 4 betroffen ist. Danach folgen die Gaming-Branche mit 18 % und die Hightech-Branche mit 15 %. Diese weit verbreitete Bedrohung ist wahrscheinlich auf die anhaltenden geopolitischen Spannungen zurückzuführen, insbesondere auf die Kriege zwischen Israel und der Hamas sowie zwischen Russland und der Ukraine, die zu einem Anstieg der weltweiten Hacktivismus-Aktivitäten geführt haben.

API-Wachstum löst Anstieg von DDoS-Angriffen auf Layer 7 aus

Obwohl Webanwendungen traditionell das Hauptziel von Cyberangriffen sind, konnten wir im Berichtszeitraum auffällige Spitzenwerte von Layer-7-DDoS-Angriffen auf APIs feststellen. Das liegt vor allem an der zunehmenden Einführung von APIs in Finanzdienstleistungen, mit der neue Compliance- und regulatorische Anforderungen erfüllt werden sollen. Und da sich Unternehmen stärker auf APIs verlassen, passen Cyberkriminelle ihre Taktiken an, wodurch API-Sicherheit für moderne Unternehmen eine wichtige Priorität ist.

Trafficspitzen machen deutlich, dass DDoS-Angriffe nach Frequenz und Volumen bewertet werden müssen

DDoS-Angriffe im Finanzdienstleistungssektor liefern eine wichtige Erkenntnis: Die Häufigkeit der Ereignisse korreliert nicht immer mit der Angriffsintensität. Obwohl es in manchen Monaten nur zu wenigen Angriffen kam, deuten die entsprechenden Gbit/s-Daten auf erhebliche Trafficspitzen hin, was die Notwendigkeit unterstreicht, bei der Bewertung von DDoS-Angriffsauswirkungen sowohl die Angriffshäufigkeit als auch das -volumen zu berücksichtigen.

36 %

Prozentsatz der verdächtigen Domains, die Finanzinstitute ins Visier nehmen

Phishing-Angriffe richten sich zunehmend gegen Finanzdienstleistungskunden und erhöhen das Risiko von Identitätsdiebstahl und Kontoübernahmen. Dieser Angriffstrend führt dazu, dass Finanzinstitute von den Aufsichtsbehörden genauer unter die Lupe genommen werden – und Verstöße beeinträchtigen das Vertrauen der Kunden.

30 %

Prozentsatz der Seitenbesuche, die an Phishing- und Nachahmungs-Websites weitergeleitet werden

Angreifer leiten erfolgreich Traffic an betrügerische Websites um, indem sie legitime Websites und Apps für Finanzdienstleistungen imitieren. Sie nehmen weiterhin mit Phishing Finanzinstitute ins Visier, um an die vielen sensiblen Daten zu gelangen, die sich in diesen Organisationen befinden.

Finanzdienstleistungen bleiben das wichtigste Ziel für Layer-3- und Layer-4-DDoS-Angriffe

Layer-3- und Layer-4-DDoS-Angriffe zielen auf Netzwerk- und Transportschichten ab, wodurch die Netzwerkinfrastruktur überlastet und Serverressourcen sowie Bandbreite erschöpft werden. Diese Angriffe senden eine enorme Menge an Traffic, mit dem Ziel, Netzwerkkapazitäten zu beanspruchen und die Performance für legitime Nutzer zu beeinträchtigen. Unter allen Branchen war die Finanzdienstleistungsbranche das primäre Ziel für Layer-3- und Layer-4-DDoS-Angriffe (Abbildung 1). Dieser Trend wird von mehreren, miteinander verbundenen Faktoren angetrieben, die für Schwachstellen sorgen und optimale Chancen für Angreifer schaffen.

DDoS-Angriffsereignisse auf Layer 3 und 4 nach Branche

1. Januar 2023 bis 30. Juni 2024

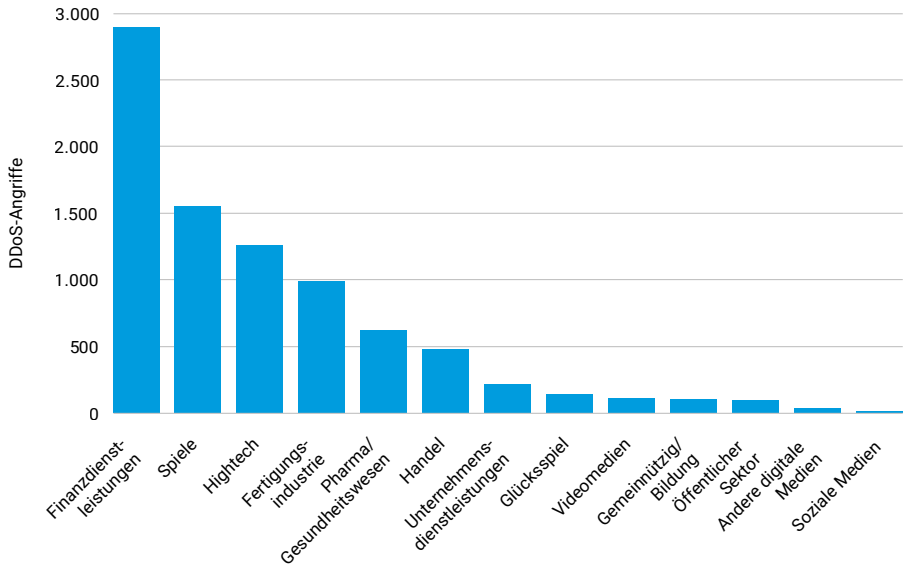


Abb. 1: Die Finanzdienstleistungsbranche liegt bei DDoS-Angriffen auf Layer 3 und 4 weit vor anderen Branchen.

Geopolitische Spannungen haben bei der Zunahme von DDoS-Angriffen auf Finanzinstitute eine bedeutende Rolle gespielt. Der anhaltende russisch-ukrainische Krieg sowie der Krieg zwischen Israel und der Hamas verursachten einen deutlichen Anstieg des pro-russischen und pro-palästinensischen Hacktivismus. Diese Konflikte haben einen Anstieg der DDoS-Angriffe ausgelöst, insbesondere auf europäische Banken mit Verbindungen zur Ukraine. Die politisch motivierte Natur dieser Angriffe erhöht die Komplexität der Bedrohungslandschaft.

Finanzinstitute sind aufgrund der weitreichenden Auswirkungen besonders attraktive Ziele für DDoS-Angreifer. Eine erfolgreiche Betriebsunterbrechung kann zu schwerwiegenden finanziellen Auswirkungen, erheblichen Rufschädigungen und einem Verlust an Vertrauen in das globale Finanzsystem führen. Das Potenzial für weitreichende Folgen macht Finanzdienstleistungen zu einem vorrangigen Ziel für diejenigen, die größtmögliche Störungen verursachen oder ein politisches Statement setzen wollen.

Technologische Fortschritte haben die Leistungsfähigkeit und die Kompetenzen von DDoS-Angreifern drastisch erhöht. Sie können nun VM-Botnets (Virtuelle Maschine) einsetzen, um Angriffe effizienter durchzuführen. Dabei nutzen sie die Rechenressourcen zahlreicher VMs und IoT-Geräte. Dieser Ansatz nutzt die verteilte Struktur von Cloud-Services und macht es schwieriger, Angriffe abzuwehren und nachzuverfolgen. Angreifer können mit hoher Bandbreitenverfügbarkeit und enormen Rechenressourcen anpassungsfähige, leistungsstarke und kostengünstige DDoS-Angriffe mit verschiedenen Strategien starten.

Die wachsende Angriffsfläche in der Finanzdienstleistungsbranche hat ebenfalls zur Zunahme von DDoS-Angriffen beigetragen. Die zunehmende Verwendung von digitalen Services und APIs hat Angreifern mehr Einstiegspunkte eröffnet. Diese Entwicklung hat die Komplexität von Finanzsystemen erhöht und zahlreiche potenzielle Schwachstellen für Angreifer geschaffen. Nicht dokumentierte Shadow-APIs sind besonders besorgniserregend. Sie sind oft ungeschützt, da Informationssicherheitsteams nicht einmal wissen, dass sie existieren. Angreifer können diese APIs ausnutzen, um Daten zu extrahieren, Authentifizierungskontrollen zu umgehen oder Störungen zu verursachen.

Angreifer können mit hoher Bandbreitenverfügbarkeit und enormen Rechenressourcen anpassungsfähige, leistungsstarke und kostengünstige DDoS-Angriffe mit verschiedenen Strategien starten.

Auch der Druck durch Regulierungsbehörden hat die Anfälligkeit von Finanzinstituten für DDoS-Angriffe unbeabsichtigt erhöht. Anforderungen wie die von der Europäischen Union eingeführte Zahlungsdiensterichtlinie 2 (PSD2) haben dazu geführt, dass Banken ihre Systeme über APIs für Dritte öffnen, beispielsweise für Fintech-Unternehmen. So können Banken durch die Integration von Fintech, mobilen Apps und anderen Plattformen auf steigende Kundenerwartungen reagieren. Doch hierdurch werden auch die Sicherheitsrisiken erhöht und die Angriffsflächen vergrößert. Die stärkere Verwendung von APIs in diesen verschiedenen Unternehmen schafft mehr potenzielle Points of Failure für Angreifer.

Insgesamt haben diese Faktoren dafür gesorgt, dass die Finanzdienstleistungsbranche weiterhin das Hauptziel für Layer-3- und Layer-4-DDoS-Angriffe ist. Die Kombination aus geopolitischen Motivationen, hochwertigen Zielen, technologischen Fortschritten, einer wachsenden digitalen Präsenz und regulatorischem Druck hat ein Umfeld geschaffen, in dem DDoS-Angriffe auf Finanzinstitute nicht nur häufiger vorkommen, sondern auch potenziell schädlicher sind als je zuvor. Im Zuge der Weiterentwicklung der Branche muss sie auch ihre Abwehrmaßnahmen gegen diese immer komplexeren und hartnäckigeren Bedrohungen verbessern.

DDoS-Angriffsereignisse auf Layer 3 und 4: Eine Achterbahnfahrt

Obwohl in der Finanzdienstleistungsbranche die höchste Häufigkeit von Layer-3- und Layer-4-DDoS-Angriffen auftritt, schwankt die Rate dieser Angriffe im Jahresverlauf (Abbildung 2).

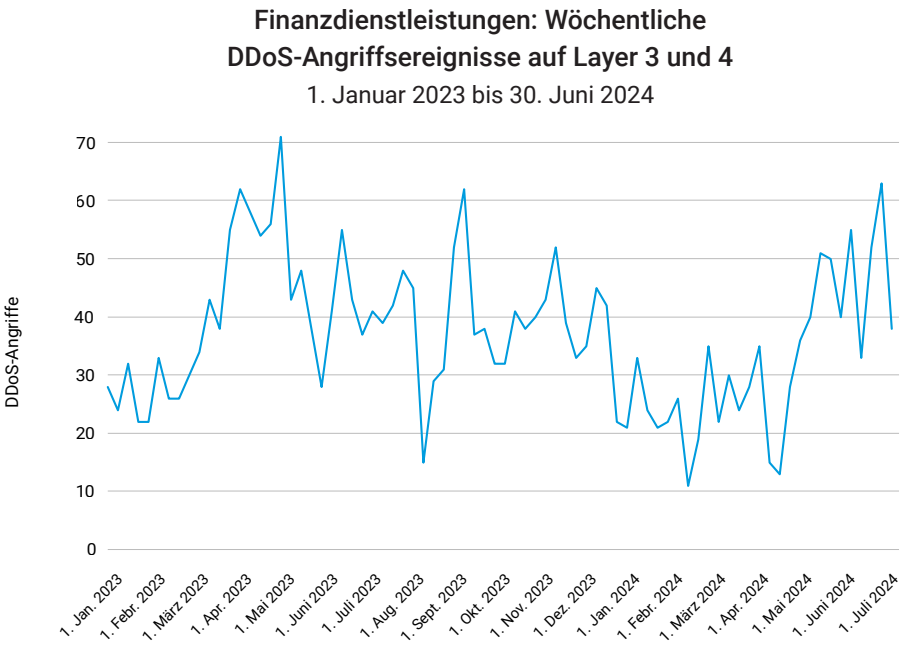


Abb. 2: Anstieg und Rückgang von Layer-3- und Layer-4-DDoS-Angriffen in der Finanzdienstleistungsbranche

Die Layer-3- und Layer-4-DDoS-Angriffe auf die Finanzdienstleistungsbranche im März/April 2023, August/September 2023 und April/Mai 2024 können mehreren spezifischen Faktoren zugeschrieben werden.

Im Frühjahr läuft von März bis April die US-Einkommensteuersaison, die DDoS-Angreifern eine attraktive Chance bietet. Ab dem 16. April – der mit dem Zeitpunkt zusammenfällt, an dem viele Banken ihre Gewinne im ersten Quartal melden – stieg der Kontomissbrauch bei nationalen und regionalen Banken spürbar an. In dieser Zeit berichteten auch IAM- (Identity and Access Management) und Netzwerkanbieter wie Okta und Cisco von verstärkten und erheblichen Credential-Stuffing-Angriffen, die auf Online-Services abzielten.

Im April 2023 trug wahrscheinlich die Entdeckung der schwerwiegenden Sicherheitslücke im Service Location Protocol (SLP) (CVE-2023-29552) zu dem Anstieg der Angriffsaktivitäten bei. Diese Schwachstelle, die DDoS-Angriffe sowohl auf Netzwerk- als auch auf Anwendungsebene verstärken kann, betrifft Berichten zufolge mehr als 2.000 Unternehmen weltweit und mehr als 54.000 SLP-Instanzen im gesamten Internet. Durch Ausnutzung dieser Schwachstelle könnten Angreifer die kompromittierten Instanzen nutzen, um großangelegte DDoS-Verstärkungsangriffe durchzuführen. Mit einem bis zu 2.200-fachen Verstärkungsfaktor hat diese Schwachstelle einen der bedeutendsten Verstärkungsangriffe ermöglicht, die jemals dokumentiert wurden.

Wir haben ein wichtiges Ereignis identifiziert, indem wir den Zeitraum August/September 2023 untersucht haben. Akamai beobachtete und vereitelte am 5. September 2023 den größten aufgezeichneten DDoS-Angriff auf ein US-Finanzinstitut. Dieser Angriff kombinierte ACK-, PUSH-, RESET- und SYN-Flood-Techniken und erreichte Spitzenintensitäten von 633,7 Gigabit pro Sekunde (Gbit/s) und 55,1 Millionen Paketen pro Sekunde (Mpps). Trotz seiner hohen Intensität war der Angriff kurz: Er dauerte weniger als zwei Minuten.

Sicherheit im Fokus

Intensität von DDoS-Angriffen auf Layer 3 und 4: Ereignisse im Vergleich zu Gbit/s

Um die Bedrohung, die DDoS-Angriffe für die Finanzdienstleistungsbranche darstellen, vollständig zu erfassen, ist es entscheidend, ihre Komplexität und Größe zu verstehen. Hier handelt es sich nicht um einfache, isolierte Vorfälle: Jeder Angriff umfasst oft mehrere Versuche mit hohem Datenvolumen, die Netzwerke mit Gigabit an Daten und Millionen von Paketen pro Sekunde überschwemmen. Die Ausgereiftheit, Intensität und Dauer der Attacken nehmen zu und die Angreifer verwenden vielfältigere Techniken, die das Risiko für Finanzinstitute eskalieren lassen (Abbildung 3).

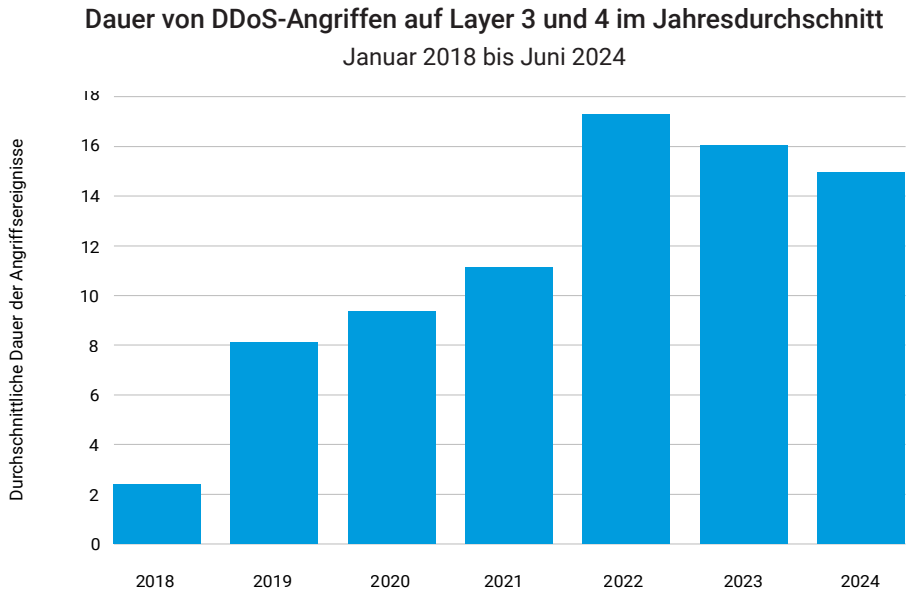


Abb. 3: Der globale Trend bei der Dauer von Layer-3- und Layer-4-DDoS-Angriffen ist steigend.

Wenn Sie darüber hinaus das Diagramm mit der Anzahl von Layer-3- und 4-DDoS-Angriffsereignissen in der Finanzdienstleistungsbranche mit den entsprechenden DDoS-Gbit/s-Daten vergleichen, werden Sie eine erhebliche Diskrepanz feststellen (Abbildung 4). Das Gbit/s-Diagramm zeigt starke Zuwächse, die sich nicht im Diagramm der Angriffsereignisse widerspiegeln. Diese Diskrepanz weist auf einen wichtigen Punkt hin: Selbst in einem Monat mit relativ wenigen Angriffsereignissen kann es immer noch zu einem extrem hohen DDoS-Traffic in Gbit/s kommen.

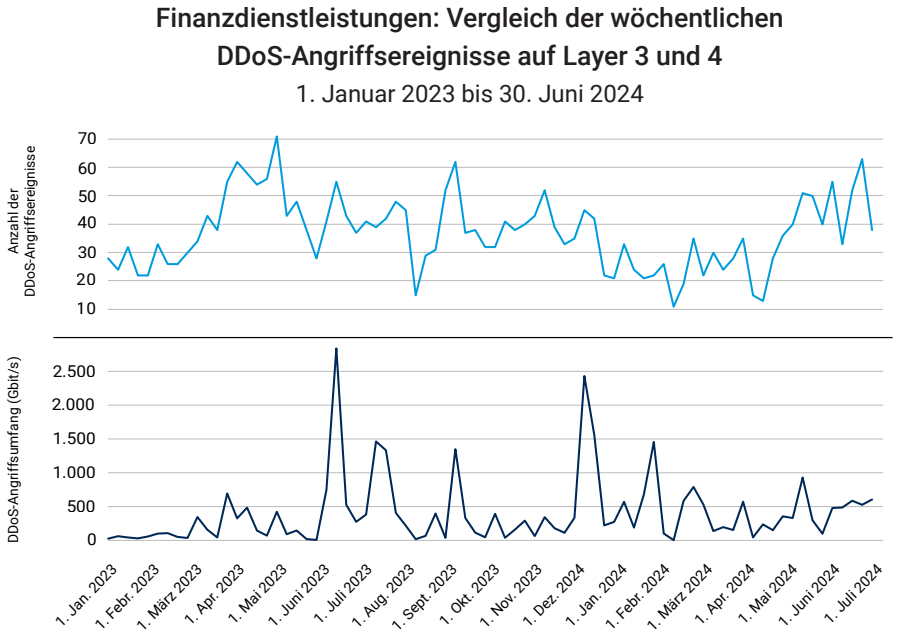


Abb. 4: Layer-3- und Layer-4-DDoS-Angriffsereignisse in der Finanzdienstleistungsbranche im Vergleich zu den Messungen in Gbit/s

Diese Beobachtung macht etwas Entscheidendes deutlich: Wenn wir uns lediglich auf die Häufigkeit der Angriffsereignisse konzentrieren, wird die wahre Bedrohung erheblich unterschätzt. Es ist wichtig, sowohl das Volumen als auch die Intensität des Datenverkehrs bei jedem Angriff zu berücksichtigen. Eine kleine Anzahl hochintensiver DDoS-Angriffe kann weitaus mehr Schaden anrichten als eine größere Anzahl kleinerer Ereignisse. Daher ist es unerlässlich, den gesamten Umfang jeder Bedrohung zu bewerten.

Die Tendenz geht hin zu einem Vektor: Layer-3- und Layer-4-DDoS-Angriffe im Finanzdienstleistungssektor, bei denen nur ein Vektor genutzt wurde

Multi-Vektor-Angriffe auf Anwendungen oder Netzwerke sind eine gängige Strategie für Cyberkriminelle, die versuchen, ein System zu schädigen oder sich unbefugten Zugriff zu verschaffen. Angreifer, die sich auf die Finanzdienstleistungsbranche konzentrieren, unternehmen jedoch häufiger Attacken mit einzelnen Vektoren, wenn es um DDoS auf Layer 3 und 4 geht (Abbildung 5).

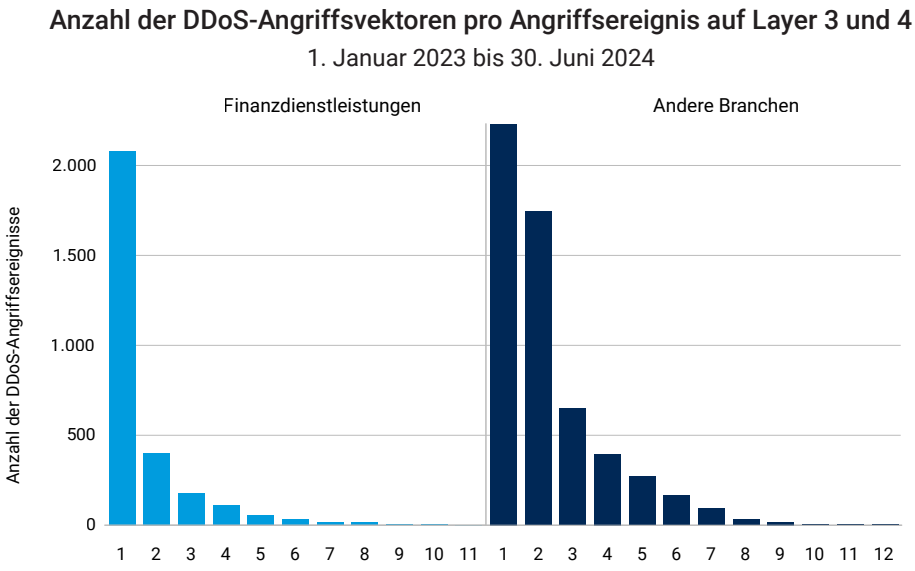


Abb. 5: Bei Layer-3- und Layer-4-DDoS-Angriffen in der Finanzdienstleistungsbranche kommt häufiger nur ein Vektor zum Einsatz.

DDoS-Angriffe mit nur einem Vektor, die auf Layer 3 und 4 abzielen, erfordern weniger Ressourcen und können auch für sich genommen äußerst effektiv sein – insbesondere gegen Finanzinstitute, die über eine leistungsstarke Abwehr gegen komplexere Angriffe verfügen. Sie sind im Allgemeinen einfacher auszuführen und erfordern weniger Koordination als Multi-Vektor-Angriffe. Möglicherweise gibt es auch einige bekannte spezifische Schwachstellen von Finanzinstituten auf Layer 3 und 4, die mit einem einzigen Angriffsvektor wirksam ausgenutzt werden könnten – ohne das Risiko, das mit anderen Angriffsvektoren einhergeht, die von Sicherheitsmaßnahmen entdeckt werden könnten.

Diese Vorliebe für Angriffe mit einzelnen Vektoren in der Finanzdienstleistungsbranche stellt Cybersicherheitsteams vor eine einzigartige Herausforderung: Sie müssen gegenüber komplexen Angriffen mit mehreren Vektoren wachsam bleiben, aber auch sicherstellen, dass jede Verteidigung konzentrierten Ein-Vektor-Angriffen auf Layer 3 und 4 standhalten kann.

Zunehmende Layer-7-DDoS-Angriffe auf APIs

DDoS-Angriffe auf Anwendungsebene (Layer 7), die auch als HTTP- oder Web-Traffic-Angriffe bezeichnet werden, haben sich stark verbreitet und sind heute eine bevorzugte Methode für Cyberkriminelle, die die Finanzdienstleistungsbranche ins Visier nehmen. Diese Angriffe konzentrieren sich insbesondere auf die ressourcenintensiveren Komponenten von Anwendungen, wodurch legitimen Nutzern der Zugriff verweigert wird. Im Gegensatz zu DDoS-Angriffen auf Layer 3 und 4, die häufig durch Firewalls und Netzwerkschutz abgewehrt werden, umgehen Layer-7-Angriffe diese Abwehrmechanismen: Sie geben sich als legitime Anfragen aus, wenn sie bestimmte Anwendungsseiten oder Suchfunktionen ins Visier nehmen, um den Anwendungsserver zu überfordern.

Obwohl Webanwendungen in der Finanzdienstleistungsbranche im Allgemeinen häufiger angegriffen wurden als APIs, haben wir einen starken Anstieg von Layer-7-DDoS-Angriffen beobachtet, die speziell auf APIs abzielen (Abbildung 6). Diese Spitzen sind ausgeprägter und vielfältiger als das allgemeine API-Angriffsmuster in anderen Branchen.

Finanzdienstleistungen: Tägliche Layer-7-DDoS-Angriffe

1. Januar 2023 bis 30. Juni 2024

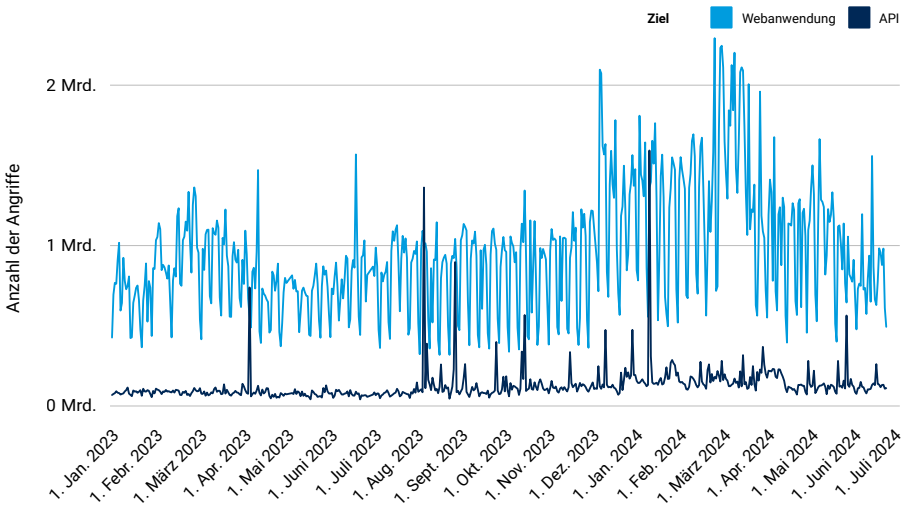
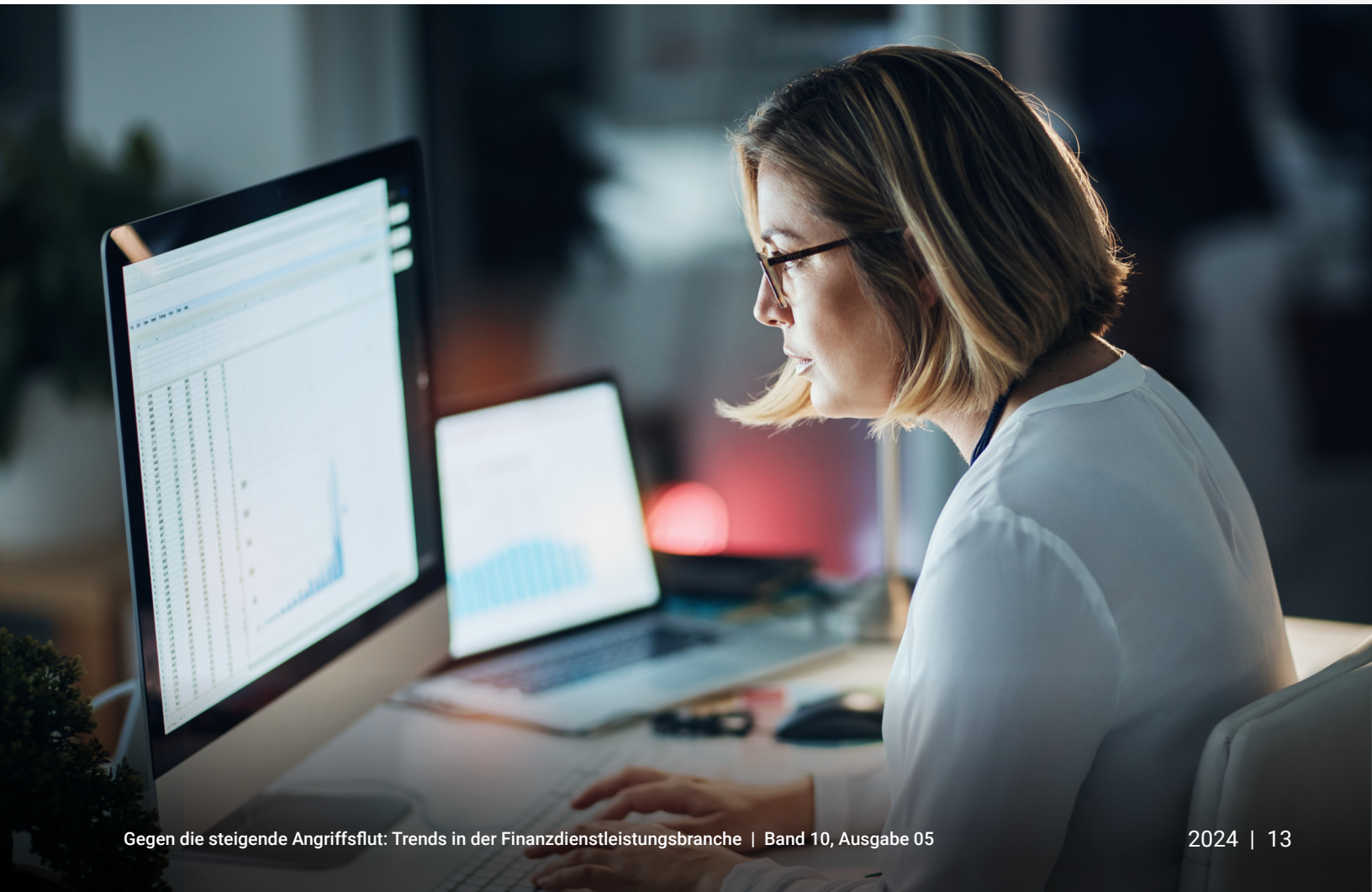


Abb. 6: Bei Layer-7-DDoS-Angriffen auf Finanzdienstleister unterscheiden sich die Angriffsmuster zwischen Webanwendungen und APIs erheblich.

Diese starken Zuwächse traten insbesondere im April und August 2023 sowie im Januar 2024 auf. Wir schreiben diese Spitzen ähnlichen Faktoren zu, wie sie auch Layer-3 und Layer-4-Angriffe beeinflussen. Es gibt jedoch noch einige zusätzliche Layer-7-spezifische Faktoren.

Angreifer suchen ständig nach neuen Schwachstellen, die sie ausnutzen können, und die Entdeckung solcher Schwachstellen kann zu plötzlichen Angriffszunahmen führen. So ermöglichte beispielsweise die „HTTP/2 Rapid Reset"-Sicherheitsanfälligkeit (CVE-2023-44487), die erstmals im August 2023 identifiziert wurde, hocheffektive Layer-7-DDoS-Angriffe. Diese Schwachstelle ermöglichte es Angreifern, eine scheinbar harmlose Logik auszunutzen und mehrere Anfragen in einem Stream zu bündeln, was Server und Anwendungen überforderte. Das führte zu dem bisher größten aufgezeichneten Layer-7-DDoS-Angriff.

Darüber hinaus bleiben saisonale DDoS-Angriffe eine beliebte Taktik für Cyberkriminelle, die es auf Finanzinstitute abgesehen haben – mit deutlichen Spitzen während der Steuer- und Urlaubssaison. Der deutliche Anstieg im Januar 2024 nach der hektischen Weihnachtszeit deutet darauf hin, dass Angreifer darauf vorbereitet waren, in Zeiten erhöhter Online-Transaktionen zur Tat schreiten.



Ransomware und Hacktivismus in der Finanzdienstleistungsbranche

Die Finanzdienstleistungsbranche wird häufig von raffiniert vorgehenden Cyberkriminellen wie Ransomware-Gruppen angegriffen. Diese Gruppen setzen eine Vielzahl von Techniken ein, um Finanzinstitute zu infiltrieren, vertrauliche Informationen zu stehlen und hohe Lösegelder zu verlangen. Obwohl die Angriffe hauptsächlich finanzielle Ziele verfolgen, können sie auch mit dem geopolitischen Kontext zusammenhängen. Das kann der Fall sein, wenn Finanzinstitute angegriffen werden, weil sie bestimmte politische Verbindungen haben. So war es bei der russischen Ransomware-Gruppe REvil (auch bekannt als Sodinokibi) oder auch bei BlackCat (ALPHV), wie der Angriff der Gruppe auf eine bekannte Bank gezeigt hat.

Eine der aktivsten Ransomware-Gruppen, die für ihre Angriffe auf große Unternehmen bekannt ist (einschließlich Finanzinstituten), ist weiterhin LockBit – und das trotz der jüngsten Strafverfolgungsmaßnahmen gegen die Gruppe. Die Operation Cronos, an der sich im Rahmen einer neuartigen internationalen Taskforce auch Europol und Eurojust beteiligten, konnte LockBit durch eine neue Infrastruktur überwinden. Die Ransomware-Gruppe kam zurück mit einer neuen Infrastruktur und einer Dark-Web-Leaksite, und das nur wenige Tage nachdem die Strafverfolgungsbehörden im Februar 2024 die Server der Gruppe beschlagnahmt hatten. LockBit erklärte, dass es als Reaktion auf die Operation Cronos mit verstärkten Angriffen auf Regierungsnetzwerke zurückschlagen werde.

Auch die Ransomware-Gruppe CL0P ist weiterhin aktiv. Sie ist vor allem dafür bekannt, Schwachstellen in Dateiübertragungssoftware auszunutzen, die in Unternehmen wie Finanzinstituten weit verbreitet ist. Ein bemerkenswertes Beispiel war die Zero-Day-Sicherheitslücke CVE-2023-34362. Sie betraf die MOVEit Transfer-Software und begann mit einer SQL-Injection, mit der die MOVEit Transfer-Webanwendung infiltriert werden konnte. Mindestens 15 Banken und Kreditgenossenschaften meldeten Datenschutzverletzungen infolge der MOVEit-Schwachstelle. CL0P hat sich auch durch andere Techniken wie Phishing Erstzugang verschafft und wird weiterhin als RaaS-Modell (Ransomware-as-a-Service) betrieben. In jüngster Zeit hat die Gruppe ihre Taktik weiterentwickelt, um Ziele wie Finanzinstitute gleich vierfach zu erpressen. Zusätzlich zu den Techniken der dreifachen Erpressung umfasst die vierfache Erpressung das Senden von Nachrichten an Geschäftspartner, Mitarbeiter, Kunden, hochrangige Führungskräfte und Medien, um sie darüber zu informieren, dass das Unternehmen gehackt wurde. Und diese Taktik hat zu einem Anstieg der durchschnittlichen Ransomware-Zahlungen geführt.

Andere hacktivistische Bedrohungsakteure, die Finanzinstitute im Visier haben, aber nicht als Ransomware-Gruppen eingestuft werden, sind Anonymous Sudan, KillNet und NoName057(16). Sie alle sind für ihre Aktivitäten im Zusammenhang mit dem russisch-ukrainischen Krieg bekannt und Anonymous Sudan hat darüber hinaus erklärt, sich als Reaktion auf den Krieg zwischen Israel und der Hamas an Cyberangriffen beteiligt zu haben. Im vergangenen Jahr nutzten diese Gruppen – zusätzlich zu zahlreichen anderen Gruppen von Bedrohungsakteuren – das Chaos aus, das durch den Russland-Ukraine-Krieg ausgelöst wurde, und richteten ihre Aufmerksamkeit auf die kritische Bankeninfrastruktur.

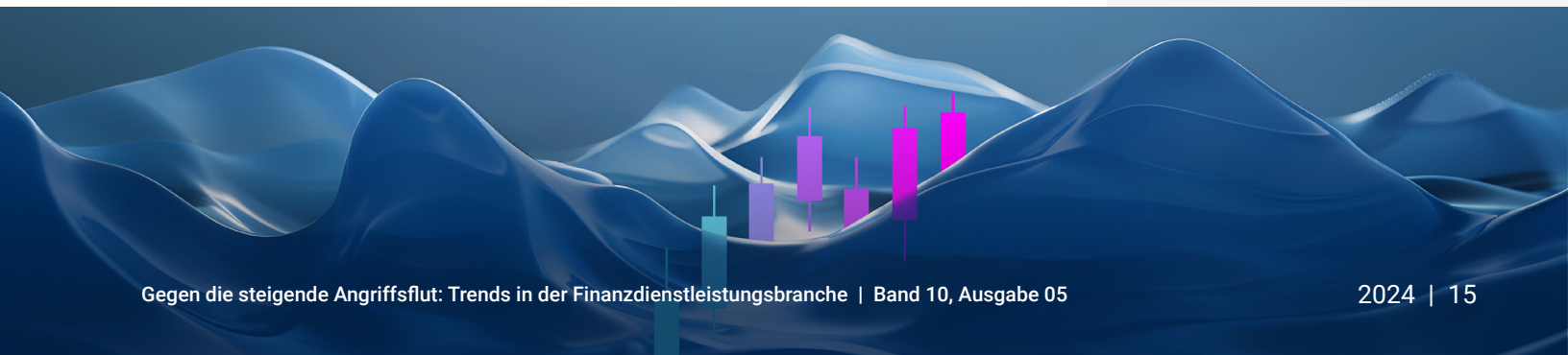
Es gibt viele andere sehr aktive Bedrohungsakteure, die zwar nicht als Ransomware-Gruppen klassifiziert werden, aber dafür bekannt sind, Finanzdienstleister anzugreifen. Dazu gehören die Lazarus Group, MoneyTaker, Carbanak/FIN7, Cobalt und APT41.

Angesichts der anhaltenden Bedrohungen, die von diesen Akteuren ausgehen, ist es für Finanzinstitute von entscheidender Bedeutung, sich der aktuellen Bedrohungssituation bewusst zu sein. Sie müssen die Motivationen und Techniken der Angreifer besser verstehen, um wirksamere Verteidigungsstrategien zu entwickeln. Empfohlene Schutzmaßnahmen finden Sie im Abschnitt zur Risikominderung weiter unten in diesem Bericht.

Jüngster Ausbruch von DDoS-Hacktivismus bei Finanzinstituten im Nahen Osten

Die Finanzdienstleistungsbranche im Nahen Osten hat in jüngster Zeit einen Anstieg ausgeklügelter und anhaltender DDoS-Angriffe erlebt, die durch geopolitische Spannungen ausgelöst wurden. Dieser Trend ist besonders in der Region Europa, Naher Osten und Afrika (EMEA) zu beobachten und verdeutlicht die zunehmende Bedrohung durch politisch motivierte DDoS-Angriffe auf Finanzinstitute.

Ein bemerkenswertes Beispiel für diese Entwicklung ereignete sich Anfang des Jahres, als die pro-palästinensische Hacktivistengruppe BlackMeta (auch bekannt als DarkMeta) einen sechstägigen Layer-7-DDoS-Angriff auf ein Finanzinstitut in den Vereinigten Arabischen Emiraten (VAE) startete. Der Angriff wurde durch InfraShutdown erleichtert, einen DDoS-Dienst, der die zunehmende Zugänglichkeit dieser Angriffstools verdeutlicht. BlackMeta, das seit November 2023 aktiv ist, hat in der Vergangenheit Organisationen in Israel, den Vereinigten Arabischen Emiraten und den Vereinigten Staaten angegriffen.



Der Angriff auf das Finanzinstitut der VAE hielt nicht nur lange an, sondern erreichte auch eine erhebliche Intensität. Er erstreckte sich über etwa 100 Stunden, wobei die Anfragewellen zwischen 4 und 20 Stunden dauerten und durchschnittlich 4,5 Millionen Anfragen pro Sekunde umfassten. Die Bank wurde 70 % der Zeit aktiv angegriffen, was ihre Services erheblich beeinträchtigte. BlackMetas Kampagne gegen die Bank war Teil einer umfassenderen Aktion, um gegen die vermeintlichen Ungerechtigkeiten gegen Palästinenser und Muslime zu protestieren. Hierbei nutzte es Taktiken, die denen von Anonymous Sudan ähneln.

Glücklicherweise konnten die Abwehrmaßnahmen des Finanzinstituts eine größere Störung verhindern. Der Vorfall unterstreicht jedoch den wachsenden Trend hin zu politisch motivierten Cyberangriffen. Der Fall hebt auch die zunehmende Verfügbarkeit von DDoS-Diensten hervor, die Hacktivistengruppen großangelegte Angriffe erleichtern. Diese Entwicklung unterstreicht die Notwendigkeit leistungsstarker Cybersicherheitsmaßnahmen zum Schutz vor umfangreichen und lang anhaltenden Bedrohungen.

Ein weiterer aktueller und mutmaßlich politisch motivierter DDoS-Angriff ereignete sich am 15. Juli 2024. Er richtete sich gegen ein großes Finanzdienstleistungsunternehmen in Israel. Dieser massive Angriff, der von einem global verteilten Botnet ausging, dauerte fast 24 Stunden und erreichte einen Spitzenwert von 798 Gbit/s. Akamai konnte diesen DDoS-Angriff auf Layer 3 und 4, bei dem verschiedene Vektoren wie DNS Reflection und UDP Flood zum Einsatz kamen, erfolgreich abwehren.

Während dieses Angriffs blockierte Akamai etwa 389 Terabyte an schädlichem Traffic in einer intensiven dreistündigen Phase. Der gesamte blockierte Datenverkehr über die vollständige Dauer erreichte etwa 419 Terabyte. Die Tatsache, dass am selben Tag weitere Ausfälle bei israelischen Finanzinstituten auftraten, deutet auf einen koordinierten Angriff hin, der die zunehmende Bedrohung durch fortgeschrittene DDoS-Angriffe zusätzlich unterstreicht.

Erwähnenswert ist auch, dass dieser ressourcenstarke Aggressor in den vorherigen 90 Tagen 27 Mal denselben Finanzdienstleistungskunden angegriffen hatte. Der Kunde wurde seit dem vierten Quartal 2023 wiederholt von DDoS-Angriffen getroffen, die mit dem Krieg zwischen Israel und der Hamas zu tun hatten. Die interne DDoS-Threat-Intelligence-Gruppe von Akamai berichtet, dass Institutionen und Unternehmen in Israel im Jahr 2024 eine beispiellose Anzahl von DDoS-Angriffen erlebt haben. Diese anhaltende, aggressive Kampagne zeigt das zunehmende Ausmaß und die zunehmende Intensität dieser Bedrohungen und macht deutlich, dass Angreifer hartnäckiger und einfallsreicher werden.

Auf Vertrautheit setzen: Markenmissbrauch in der Finanzdienstleistungsbranche

Wenn Finanzdienstleister Digital-First-Ansätze anwenden, um das Kundenerlebnis, die betriebliche Effizienz, die Innovation, den Umsatz und die Transparenz zu verbessern, nutzen Cyberkriminelle das Vertrauen zwischen Unternehmen und ihren Kunden aus, indem sie Marken imitieren. Abbildung 7 zeigt Beispiele für betrügerische Websites, die bekannte Finanzinstitute nachahmen. Zwar sind Phishing und Markenimitation gängige Methoden, doch die alarmierende Anzahl betrügerischer Websites und die rasante Geschwindigkeit, mit der Angreifer neue Domains erstellen können, nachdem ihre ursprünglichen Websites offline geschaltet wurden, ist äußerst besorgniserregend. Diese rasche Verbreitung stellt eine wachsende und anhaltende Bedrohung für den Finanzdienstleistungssektor dar.

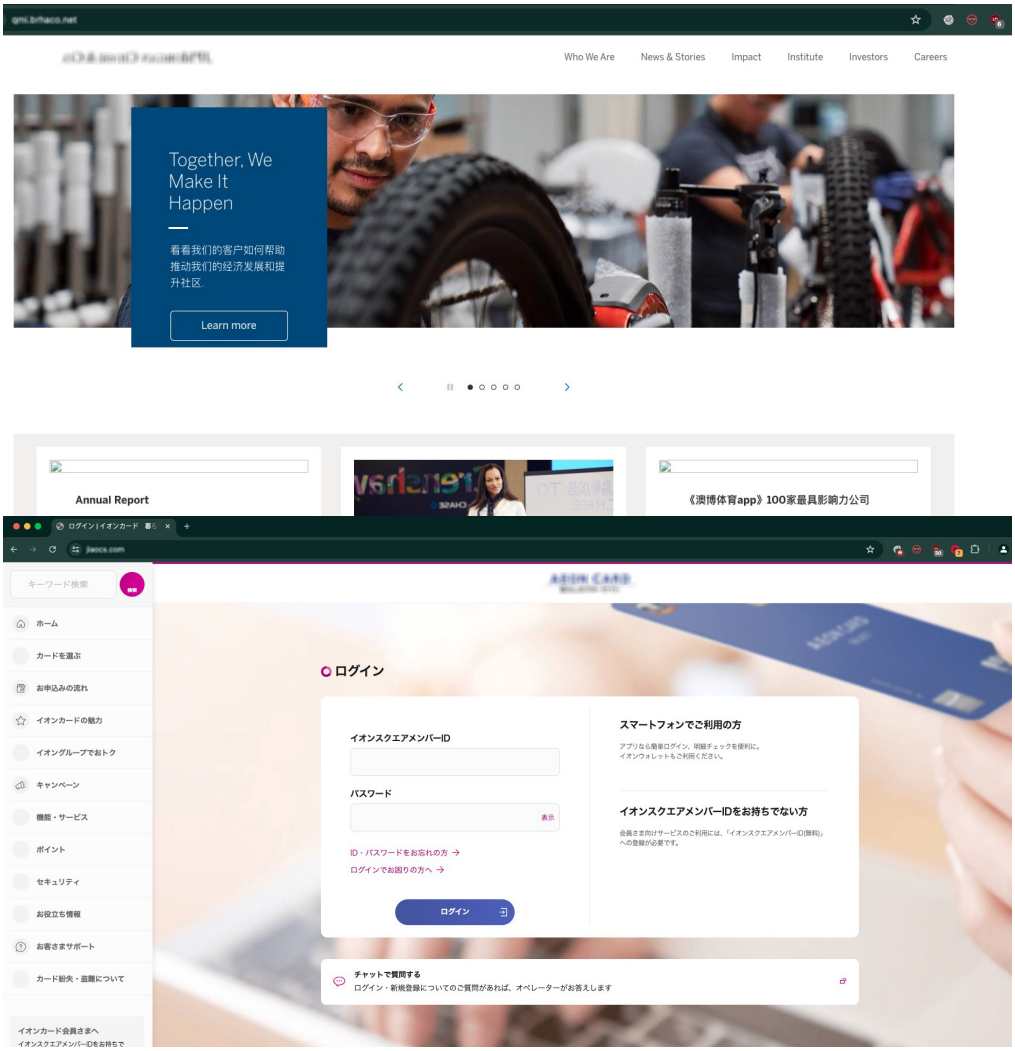


Abb. 7: Beispiele betrügerischer Phishing-Websites, die bekannte Finanzinstitute nachahmen

Die Situation in Bezug auf Markenmissbrauch hat sich durch die Entstehung von Phishing-as-a-Service-Plattformen und -Toolkits erheblich verändert. Diese Ressourcen haben die Einstiegshürde für Cyberkriminelle gesenkt, wodurch Ausmaß und Größe von Phishing-Angriffen auf Finanzdienstleister und ihre Kunden drastisch zugenommen haben. So hat die Anti-Phishing-Working Group im letzten Jahr fast fünf Millionen Phishing-Angriffe dokumentiert und 2023 als das „bisher schlimmste Phishing-Jahr" bezeichnet.

Markenmissbrauch kann auch zu weiteren Risiken führen, wie zum Beispiel Identitätsdiebstahl und Kontomissbrauch. Angreifer verkaufen Kundeninformationen oft im Dark Web oder nutzen sie zur Kontoübernahme. Im Hinblick auf die Sicherheit ist ein frühzeitiges Eingreifen bei Markenangriffen entscheidend. Indem Sie den Angriffslebenszyklus frühzeitig unterbinden, können Sie verhindern, dass Angreifer Anmeldedaten für kriminelle Zwecke ausnutzen.

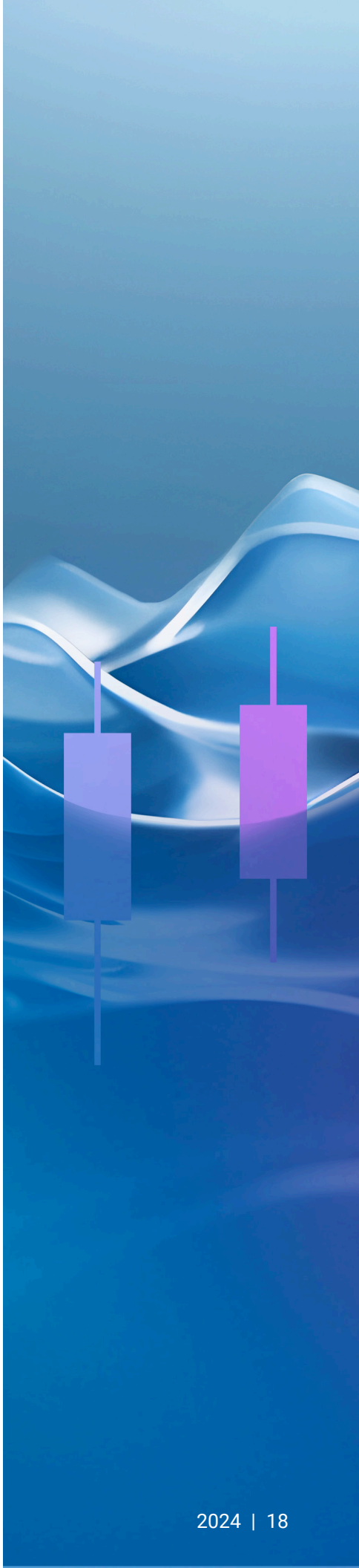
Doch die Auswirkungen von Markenmissbrauch gehen über unmittelbare Sicherheitsprobleme hinaus. Unternehmen können aufgrund von Reputationsschäden, Compliance- und rechtlichen Problemen erhebliche finanzielle Verluste erleiden. Ihnen können sogar durch gefälschte Produkte Umsätze verloren gehen. In der heutigen digitalen Landschaft ist die frühzeitige Erkennung von Markenimitationsangriffen entscheidend, um das Kundenvertrauen und die Geschäftskontinuität zu wahren.

Geschickte Täuschung: Ein genauerer Blick auf Imitationsangriffe

Sicherheitsteams stehen vor der großen Herausforderung, ihre Unternehmen vor Markenmissbrauch zu schützen, der auf verschiedenen Online-Plattformen auftreten kann. Dies macht den Schutz digitaler Assets zu einer mühseligen Aufgabe, da sowohl legitime Nutzer als auch Angreifer darauf zugreifen können. Angreifer stehlen häufig per Scraping die Inhalte öffentlich zugänglicher Assets wie Online-Banking-Portale. Sie erstellen dann ihre eigene gefälschte Website und registrieren eine falsch geschriebene Domain, um ahnungslose Nutzer zu täuschen. Darüber hinaus starten Cyberkriminelle Kampagnen über Phishing-E-Mails, Social-Media-Beiträge und andere digitale Kanäle, um potenzielle Opfer zu ihren schädlichen Websites oder gefälschten Apps zu locken.

Für diesen Bericht haben wir Markenimitationen und Phishing-Aktivitäten analysiert, die in den letzten 12 Monaten auf aktiven Domains beobachtet wurden. So wollen wir Einblicke in die Verbreitung von Markenimitationen in sämtlichen Branchen bereitstellen, jedoch mit besonderem Schwerpunkt auf Finanzdienstleistungen. Dank der umfassenden Transparenz und proprietären Lösung von Akamai sind wir zu Folgendem in der Lage:

- Traffic auf Phishing- und Markenimitations-Websites verfolgen, einschließlich Marketplaces
- Anzahl der aktiven schädlichen Domains ermitteln
- Schweregrad der schädlichen Domains bewerten



Finanzdienstleistungen waren die Branche mit den meisten Imitationen (36,25 %) unter allen Websites, die von Akamai überwacht wurden (Abbildung 8). Diese Feststellung unterstreicht die Anfälligkeit der Finanzdienstleistungsbranche für Markenimitation und -missbrauch. Unternehmen aus Handel (26,41 %) und Business Services (18,90 %) folgten auf dem zweiten bzw. dritten Platz.

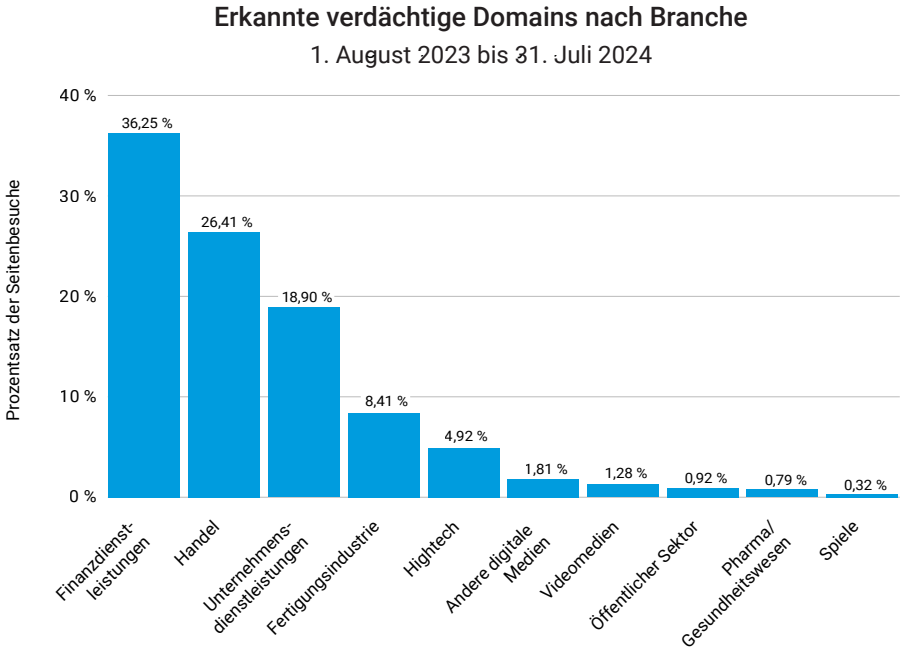


Abb. 8: Finanzdienstleistungen machten 36,3 % der Phishing- und/oder Markenimitations-Domains aus.

Die Finanzdienstleistungsbranche ist aufgrund der großen Mengen sensibler, äußerst wertvoller Daten, wie Bank- und personenbezogene Daten, ein Hauptziel für Imitationsangriffe. Mit Informationen, die Cyberkriminelle über gefälschte Bankseiten gewinnen, können sie einfach auf Konten zugreifen und diese anschließend leer räumen. Auf ähnliche Weise können sie auch andere hochwertige Finanzdaten wie Zugangsdaten für E-Wallets und Kryptowährungskonten erlangen (die Preise im Dark Web reichen von 120 bis 400 US-Dollar). Auch hier können Angreifer das Geld stehlen, das sich auf dem Konto befindet, oder die Informationen in Dark-Web-Marketplaces verkaufen. Die hohe Rendite solcher Angriffe macht Finanzdienstleister zu einem bevorzugten Ziel von Markenmissbrauch und Phishing-Angriffen.

Auch Handelsunternehmen sind seit der Verbreitung von E-Commerce und Online-Shopping zu lukrativen Zielen für Markenmissbrauch geworden. Hier haben Angreifer die Möglichkeiten, Anmeldedaten und andere persönliche Informationen zu stehlen. Fertigungsunternehmen und Drittanbieter, die Dienstleistungen anbieten, sind ebenso anfällig für Markenmissbrauch. Zwar hat die Digitalisierung das Geschäftswachstum insgesamt gefördert, doch sie ist für viele Unternehmen zu einer weichen Flanke geworden. Das hat zu einer Zunahme von Imitations- und Phishing-Angriffen geführt.

Die hohe Rendite [von Markenimitation] macht Finanzdienstleister zu einem bevorzugten Ziel von Markenmissbrauch und Phishing-Angriffen.

Unternehmen müssen wachsam bleiben und Sicherheitsmaßnahmen implementieren, um Marken und Kunden in dieser dynamischen digitalen Landschaft zu schützen. Dazu gehören eine kontinuierliche Überwachung auf Markenmissbrauch, schnelle Takedown-Verfahren für betrügerische Websites sowie die Aufklärung der Kunden, damit sie potenzielle Imitationsversuche erkennen können. Durch die Priorisierung dieser Maßnahmen können Unternehmen ihren Ruf und das Vertrauen ihrer Kunden in der immer komplexeren Bedrohungslandschaft schützen.

Finanzdienstleistungen im Fadenkreuz des Markenmissbrauchs

Um einen ganzheitlichen Überblick über die Auswirkungen von Markenimitation und Phishing zu erhalten, haben wir auch die Anzahl der Seitenbesuche auf verdächtigen Websites analysiert. Unsere Ergebnisse zeigen, dass Websites, die sich als Finanzinstitute ausgaben, 30 % der Besuche erhielten, während vermeintliche Handelsunternehmen 20 % der Besuche ausmachten (Abbildung 9). Bei diesen Ergebnissen stehen Finanzdienstleistungen und Handel stets an der Spitze – unabhängig davon, ob wir nach Anfragen oder Domains messen. Diese Beständigkeit unterstreicht, dass sie die Hauptziele für Markenmissbrauch und Nachahmung darstellen – und das aus gutem Grund.

Finanzdienstleistungen umfassen eine breite Palette an Zielen: von etablierten Banken bis hin zu kleineren Instituten mit weniger Sicherheitsressourcen. Und sie alle sind einem hohen Risiko ausgesetzt. Auch der Handel – eine Branche, die ähnlich streng reguliert wird (zum Beispiel durch den Payment Card Industry Security Standards Council) wie der Finanzdienstleistungssektor – ist aufgrund der Fülle an Kundeninformationen, über die er verfügt, mit erheblichen Risiken konfrontiert.

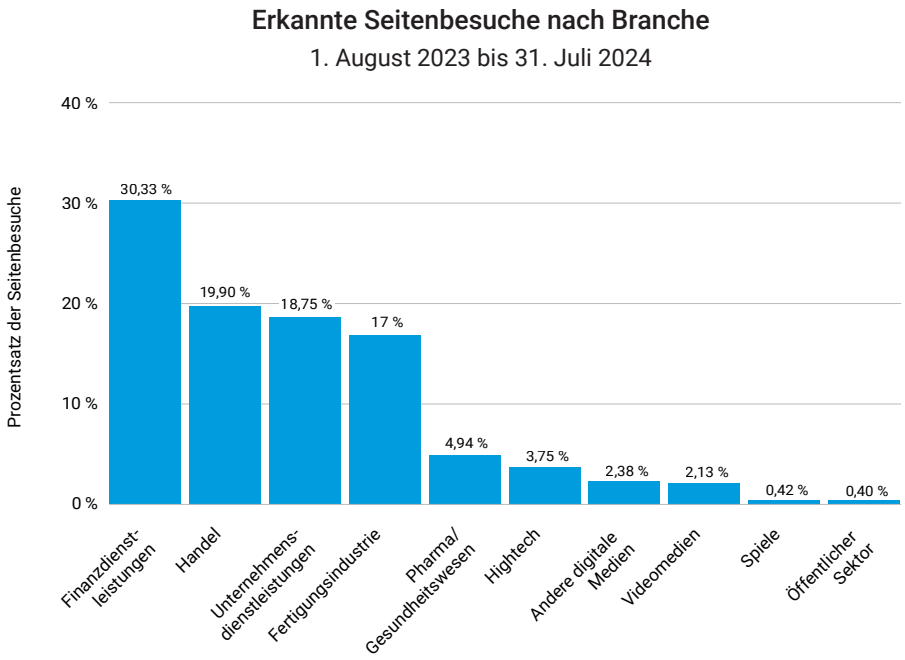


Abb. 9: Mehr als 30 % der Seitenbesuche während des Berichtszeitraums (August 2023 bis Juli 2024) betrafen verdächtige Websites, die sich als legitime Websites von Finanzdienstleistern tarnten.

Interessanterweise haben wir in den verschiedenen Branchen einige Unterschiede zwischen den Rankings der Domain-Nachahmung und den tatsächlichen Besucherzahlen festgestellt . So rangiert beispielsweise die Hightech-Branche unter den Top 5, wenn es um imitierte Domains geht, liegt aber in Bezug auf die tatsächlichen Besuche nur auf dem sechsten Platz. Ähnlich verhält es sich im Bereich Pharma/Gesundheitswesen: Hier gibt es weniger nachgeahmte Domains, doch die Zahl der Besuche bei diesen Domains ist höher.

Phishing zum Diebstahl von Zugangsdaten

Markenmissbrauch kann viele Formen annehmen. So gibt es Nachahmungswebsites, die Logo und Design eines legitimen Unternehmens exakt replizieren, oder auch betrügerische Apps und gefälschte Social-Media-Profile, die offizielle Unternehmenskonten imitieren. Um das Ausmaß dieses Problems zu verstehen, haben wir gefälschte Seiten analysiert und sie nach Typen klassifiziert: Markenimitation, Phishing, betrügerische Apps, gefälschte Shops, Paywall-Umgehungen und gefälschte Social-Media-Profile und -Shops. Es ist wichtig zu beachten, dass die Domain eines einzelnen Unternehmens basierend auf den von uns überwachten Seiten in mehrere Klassifizierungen fallen kann.

Unsere Analyse ergab, dass bei den gefälschten Domains, die auf Finanzdienstleister abzielen, Phishing dominiert, und zwar mit einem Anteil von 68 % aller erfassten Fälle (Abbildung 10). Markenimitationen stehen an zweiter Stelle und machen 24 % aller erfassten Domains aus. Auch bei den von Nutzern besuchten Websites stehen Phishing und Markenimitation an erster bzw. an zweiter Stelle. Andere Formen des Markenmissbrauchs, wie gefälschte Social-Media-Profile und Online-Shops, sind bei Finanzdienstleistern weniger wichtig als in anderen Branchen. Angriffe mit betrügerischen Apps sind zwar seltener aufgetreten, doch ist es wichtig zu beachten, dass Angreifer zunehmend kreative Methoden anwenden, um ihre Reichweite zu vergrößern.

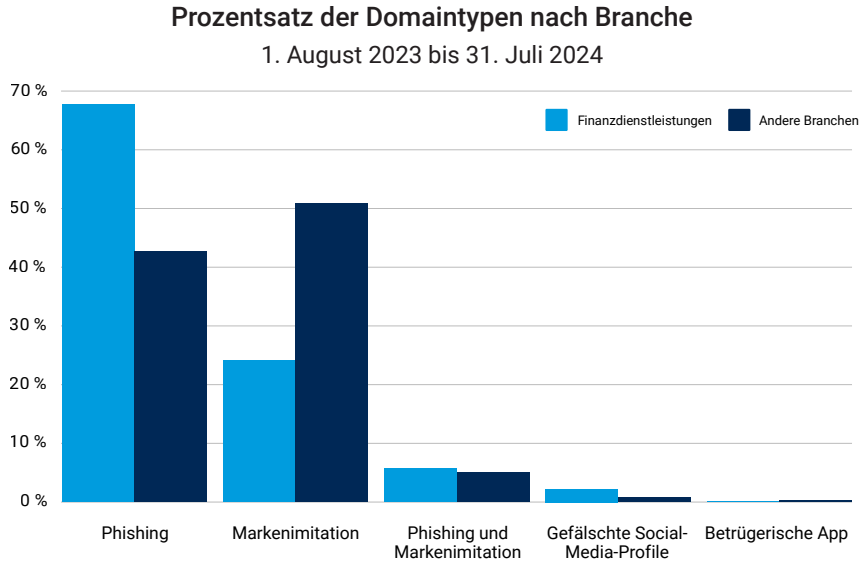


Abb. 10: Bei den meisten Domains, die wir für den Finanzdienstleistungssektor erfasst haben, handelt es sich um Phishing-Websites, deren Zahl sogar die Summe entsprechender Websites in allen anderen Branchen zusammen übertrifft.

Finanzinstitute gelten als vertrauenswürdige Unternehmen und sind damit vorrangige Ziele für Betrüger, die dieses Vertrauen ausnutzen.

Trotz des verstärkten Bewusstseins für Phishing-Risiken bleibt der Faktor Mensch nach wie vor eine erhebliche Sicherheitslücke. Das Problem verschärft sich noch durch ausgeklügelte Techniken, die von Angreifern eingesetzt werden (weitere Informationen finden Sie im Abschnitt Die Anatomie des Markenmissbrauchs). Dadurch ist es für ungeschulte Augen schwierig, eine gefälschte Seite zu erkennen. Finanzinstitute gelten als vertrauenswürdige Unternehmen und sind damit vorrangige Ziele für Betrüger, die dieses Vertrauen ausnutzen. Indem sie sich als solche Institutionen ausgeben, bringen Angreifer Nutzer dazu, ihre Anmeldedaten freiwillig zu übergeben. Sie nutzen den Ruf der Einrichtung, um ihre Betrugsversuche überzeugender und effektiver zu gestalten.

Um sowohl Unternehmen als auch ihre Kunden zu schützen, ist es wichtig, Sicherheitstechnologien mit Markenüberwachungsfunktionen zu verwenden, die proaktiv jede unbefugte Nutzung der Marke erkennen können – sei es ein Domainname, eine mobile App oder eine E-Mail-Kommunikation. Sobald diese identifiziert sind, besteht der nächste Schritt in der Durchführung von Takedowns, um den Traffic zu unterbinden, der die Kunden potenziell den Gefahren (z. B. Datendiebstahl) aussetzt, die durch Markenmissbrauch und Phishing entstehen können.

Fallstudie: Die zunehmende Komplexität von Credential-Stuffing-Angriffen auf Finanzinstitute

Ein US-amerikanisches Fintech-Unternehmen war in den Jahren 2023 und 2024 von unablässigen Credential-Stuffing-Angriffen betroffen, die auf eine seiner kundenorientierten Anwendungen abzielen. Das Ausmaß dieser Angriffe ist erschreckend: Während eines Zeitraums von 24 Stunden hat Akamai mehr als 3.000 Warnungen von verschiedenen IP-Adressen erkannt, die allesamt versuchten, Konten mit gestohlenen Anmeldedaten zu infiltrieren. Wir haben festgestellt, dass eine einzelne IP-Adresse mindestens 115 Kombinationen aus Nutzername und Kennwort verwendete. Insgesamt haben wir im Juli 2024 mehr als 100.000 Warnmeldungen registriert.

Betrügerische Finanzdienstleistungsseiten auf kritischer Risikostufe

Die Kombination aus den exklusiven Informationen unseres globalen Edge-Netzwerks sowie zusätzlichen Threat-Intelligence-Feeds von Drittanbietern verschafft uns einen deutlichen Vorteil bei der Erkennung von Markenimitationen. Wir verwenden dieses umfassende System, um jede Domain auf Grundlage ihrer Bedrohungsbewertung sorgfältig zu untersuchen und zu klassifizieren.

Wir berechnen die Bedrohungsbewertung anhand von drei Schlüsselfaktoren:

1. **Der Konfidenzwert** – unsere Gewissheit, ob ein Ereignis ein Phishing-Versuch ist
2. **Der Schweregrad** – der Grad des Risikos (kritisch, hoch, mittel oder niedrig), der mit einem Ereignis verknüpft ist
3. **Der Häufigkeitsfaktor** – die Anzahl der Ereignisse/Sitzungen, die innerhalb eines bestimmten Zeitrahmens mit der Website verknüpft sind

Unser Bewertungssystem berücksichtigt diese drei Faktoren: Konfidenz, Schweregrad und Häufigkeit. Wir kombinieren diese Werte, um für jede verdächtige Domain eine umfassende Bedrohungsbewertung zu generieren, deren Obergrenze der Wert 99 ist. So gewährleisten wir eine ganzheitliche Bewertung potenzieller Bedrohungen.

Unsere jüngste Analyse zeigt, dass der Finanzdienstleistungssektor einen alarmierenden mittleren Bedrohungswert von 85 aufweist, was die erheblichen Risiken verdeutlicht, denen die Branche nach wie vor ausgesetzt ist (Abbildung 11). Finanzinstitute stehen damit voll im Visier von Cyberkriminellen, die unablässig die riesigen Bestände an sensiblen Daten im Visier haben.

Bedrohungsbewertungen nach Branche

Branche	Mittlere Bedrohungsbewertung	Branche	Mittlere Bedrohungsbewertung
Öffentlicher Sektor	**95**	Gaming	**65**
Finanzdienstleistungen	**85**	Fertigungsindustrie	**64**
Unternehmensdienstleistungen	**85**	Andere digitale Medien	**62**
Pharma/Gesundheitswesen	**85**	Handel	**61**
Videomedien	**71**	Hightech	**60**

Abb. 11: In unserer Berechnung der mittleren Bedrohungswerte erreichen Finanzdienstleistungen einen alarmierend hohen Wert.

Während der öffentliche Sektor – wahrscheinlich aufgrund seiner Fülle an sensiblen Informationen und seiner begrenzten Sicherheitsressourcen – die höchsten mittleren Bedrohungswerte verzeichnete, sind Finanzdienstleistungen ein ebenso attraktives Ziel, da Angreifer von den enormen potenziellen Gewinnen angezogen werden. Sektoren wie Business Services und Pharma/Gesundheitswesen schneiden weisen ähnliche Bewertungen auf, was darauf hindeutet, dass Cyberkriminelle ihre Ziele diversifizieren. Aufgrund der kritischen Natur ihrer Daten bleiben Finanzinstitute jedoch weiterhin stark im Fokus.

Diese hohe Bedrohungsstufe erfordert sofortige Maßnahmen zur Stärkung der Abwehr und zur Minderung dynamischer Bedrohungen, bevor sie zu erheblichen Finanz- und Reputationsschäden führen.

Die Anatomie des Markenmissbrauchs

Das Ausmaß von Phishing- und Imitationskampagnen wird durch die Existenz von Phishing-Toolkits noch verschlimmert.

Der Erfolg von Betrug und Markenmissbrauch hängt stark davon ab, wie gut sich die Marke als Social-Engineering-Köder eignet. Angreifer nutzen das Gefühl der Vertrautheit und des inhärenten Vertrauens, das Verbraucher bekannten Marken entgegenbringen. Hierzu entwickeln sie gefälschte Websites, die legitime Marken genau nachahmen. In einigen Fällen kopieren Betrüger sogar den genauen Code, sodass diese unrechtmäßigen Websites fast identisch mit den echten Websites sind. Mit dem Aufkommen generativer KI-Tools, mit denen Betrüger verräterische Rechtschreib- und Grammatikfehler beseitigen können, ist es für Verbraucher noch schwieriger geworden, zwischen authentischen und gefälschten Websites zu unterscheiden.

Das Ausmaß von Phishing- und Imitationskampagnen wird durch die Existenz von Phishing-Toolkits noch verschlimmert. Für nur 50 US-Dollar können Angreifer Phishing-Toolkits erwerben, mit denen sie überzeugende Phishing-Websites erstellen können. Das cyberkriminelle Geschäft rund um die Entwicklung und den Verkauf von Phishing-Toolkits senkt die Einstiegshürde für Phishing- und Identitätskampagnen erheblich. Kr3pto und 16Shop sind zwei Beispiele für gängige Phishing-Toolkits. Kr3pto zielte auf britische Banken ab, deren Zwei-Faktor-Authentifizierung umgangen wurde, während sich 16Shop auf große Marken wie PayPal und Amazon konzentrierte. Im August 2023 führte eine internationale Strafverfolgungsoperation zur Verhaftung der Urheber von 16Shop. Diese Fälle verdeutlichen die wachsende Raffinesse von Phishing-Angriffen, aber auch die koordinierten Bemühungen zur Bekämpfung von Cyberkriminalität.

Unterschätzt, aber effektiv: Combosquatting

Ein weiterer wichtiger Aspekt des Markenmissbrauchs ist die Verwendung von Domainnamen, die legitimen Websites stark ähneln. In der Regel registrieren Angreifer ihre Domains, nachdem sie ihre eigene Phishing-Site gekauft oder erstellt haben. Hier spielen bewährte Techniken wie Cybersquatting und seine vielen Varianten eine entscheidende Rolle. Eine gängige Taktik ist Typosquatting, bei dem Angreifer eine Domain mit einer leichten Fehlschreibung eines Firmennamens registrieren (z. B. acamai[.]com), in der Hoffnung, dass der Verbraucher einen Tippfehler macht. Eine andere Methode, Combosquatting, beinhaltet das Hinzufügen zusätzlicher Schlüsselwörter wie „support“, „login“ oder „help“ zum Domainnamen. Diese Taktik nutzt die Microsites, die häufig auf legitimen Unternehmenswebsites zu finden sind.

Nach Untersuchungen von Akamai übertrifft das Comboquatting (Hinzufügen eines Schlüsselworts) bei der Zahl aktiver Domains das Typosquatting (Hinzufügen, Entfernen oder Ersetzen eines Buchstabens), obwohl es sich beim Combosquatting um eine weniger beachtete Taktik handelt. Interessanterweise wurde „com“ als eines der wichtigsten Schlüsselwörter in betrügerischen Websites hinzugefügt.

Verteilungsmechanismus

Nachahmungs- und Phishing-Websites werden auf verschiedenen Wegen bereitgestellt und unter die Leute gebracht. Am häufigsten geschieht dies über E-Mails. Diese E-Mail-Nachrichten sehen durch die Verwendung eines legitimen Logos überzeugend aus und enthalten dringende Nachrichten, zum Beispiel Anfragen zur Aktualisierung von Kontoinformationen. Markenmissbrauch beschränkt sich jedoch nicht nur auf Websites und E-Mails. Angreifer verbreiten Bedrohungen auch über soziale Medien und erweitern so ihre Reichweite und ihre Täuschungsstrategien.

Unsichtbare Links

Es gibt noch weitere Taktiken, die es Verbrauchern erschweren, eine Nachahmungswebsite zu identifizieren – und diese Taktiken können die Erfolgsrate solcher Angriffe erhöhen. Beispielsweise lassen sich durch verkürzte URLs, QR-Codes, Bild-Hyperlinks und Textlinks in SMS-Nachrichten schädliche Links verschleiern. Im Gegensatz zu E-Mails, bei denen Spam-Filter Schutz vor diesem Missbrauch bieten, werden Betrugsversuche per Textnachricht wahrscheinlich nicht blockiert und eher gelesen oder geöffnet.

Es gibt noch weitere Taktiken, die es Verbrauchern erschweren, eine Nachahmungswebsite zu identifizieren – und diese Taktiken können die Erfolgsrate solcher Angriffe erhöhen.

Regionale Phishing- und Imitationsangriffe im Finanzdienstleistungssektor

Markenmissbrauch betrifft Unternehmen und Verbraucher weltweit, aber einige Regionen sind aufgrund der hohen Konzentration von Traffic auf Nachahmungs- und Phishing-Websites anfälliger für Betrug und Missbrauch. Unsere Analyse zeigt, dass in der EMEA-Region in den letzten 12 Monaten der meiste Traffic auf Phishing- und Imitationsseiten verzeichnet wurde. Der Wert übertrifft sogar das Volumen in Nordamerika (Abbildung 12). Dieses Ranking umfasst sowohl Finanzdienstleistungen als auch andere Branchen.

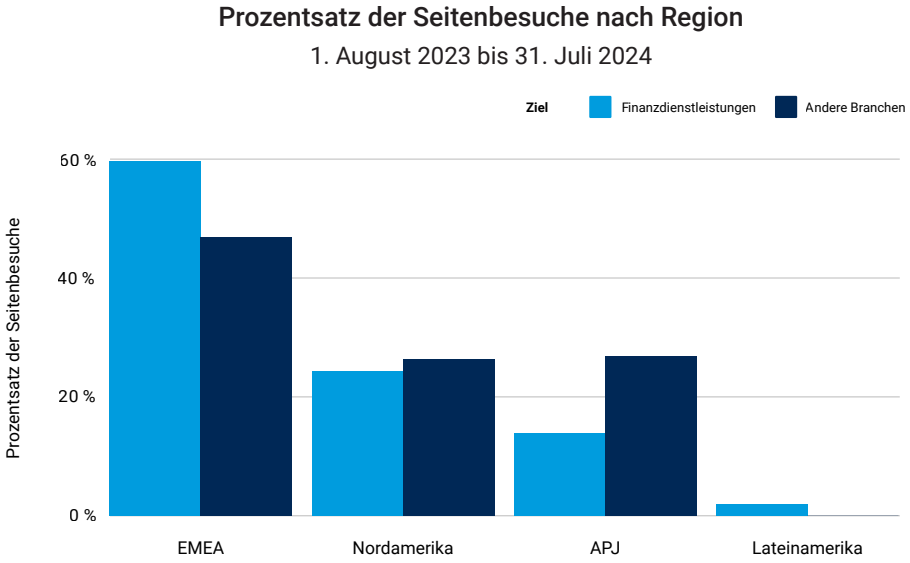
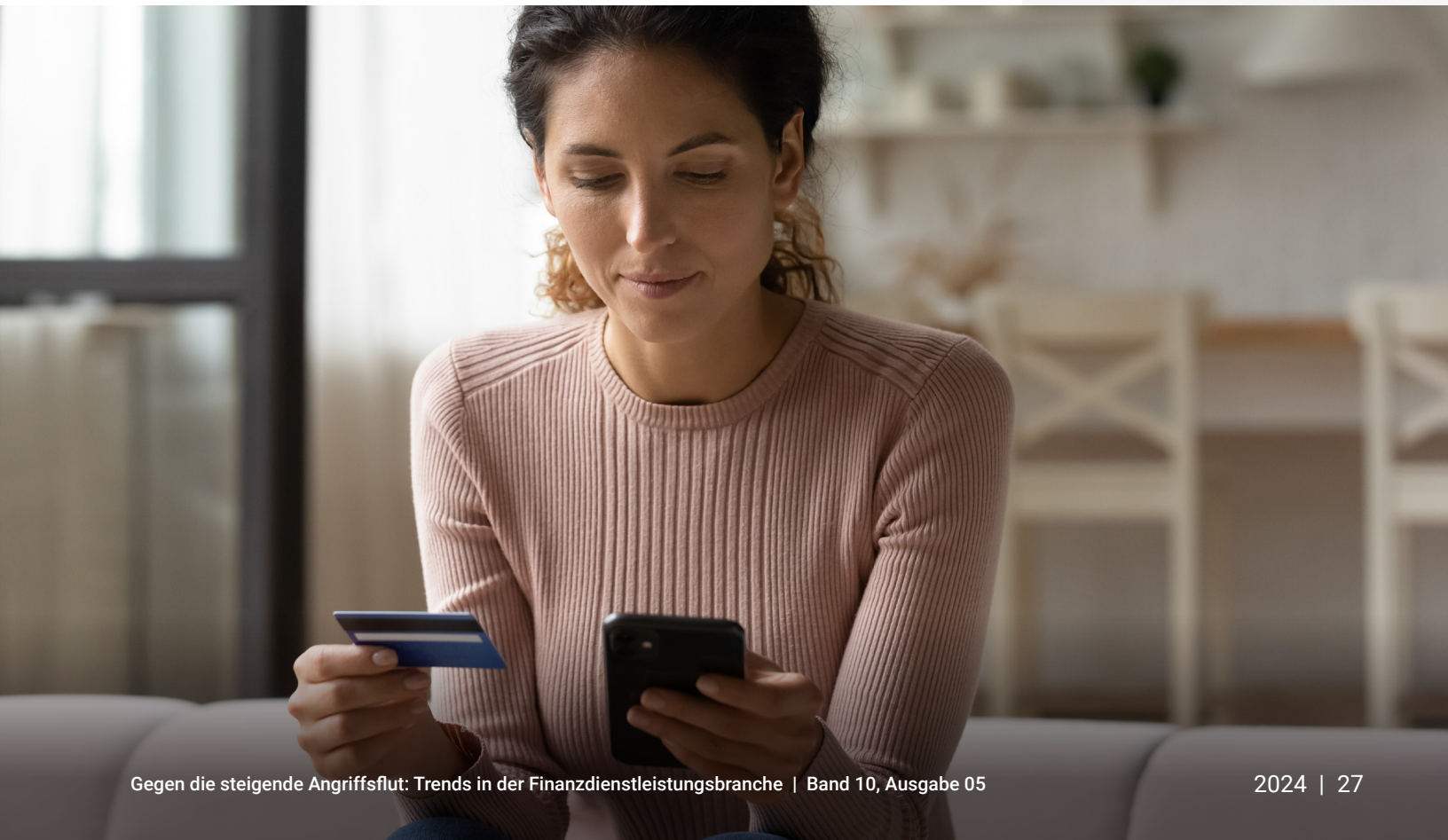


Abb. 12: EMEA übertrifft Nordamerika als Region, die am stärksten von Phishing und Markenmissbrauch im Finanzdienstleistungsbereich betroffen ist.

Obwohl in Lateinamerika und in der Region Asien-Pazifik und Japan (APJ) eine relativ geringere Anzahl von Seitenbesuchen verzeichnet wurde, bedeutet das nicht, dass hier weniger Betrugsversuche stattgefunden haben. Stattdessen spiegeln diese Ergebnisse vermutlich die hohe Konzentration globaler Marken mit großen Kundenstämmen in Nordamerika und EMEA wider. Hierdurch entsteht ein größerer Pool potenzieller Opfer für Cyberkriminelle. Wir können die Ergebnisse auch auf die Entstehung von Phishing-Toolkits wie V3B zurückführen, die seit 2023 speziell auf EU-Banken ausgerichtet sind.

Obwohl EMEA bei der Anzahl von verdächtigen Domains und Seitenbesuchen die meisten Regionen übertrifft, weist APJ die höchste mittlere Bedrohungsbewertung auf: 97. Lateinamerika erreicht trotz der geringsten Anzahl von Besuchen eine überraschende mittlere Bedrohungsbewertung von 94. Das deutet darauf hin, dass für Verbraucher sowohl in Lateinamerika als auch in APJ ein höheres Risiko besteht, dass beim Besuch von Websites Bank- und andere sensible Daten gestohlen werden.

Mehrere Faktoren tragen zum steigenden Risiko von Markenmissbrauch bei Finanzdienstleistungen in APJ bei. Erstens sind die meisten Finanzdienstleister in APJ stark digitalisiert: Fast jedes Dienstleistungsangebot kann online abgewickelt werden, ohne dass man dazu jemals eine Filiale besuchen muss. Die Internetdurchdringung und die digitale Akzeptanz in APJ sind weltweit mit am höchsten, was diese Region zu einem attraktiven Ziel für Cyberkriminelle macht. Zweitens befinden sich in dieser Region einige der aktivsten Länder der Welt, was die Social-Media-Nutzung betrifft. Finanzdienstleister haben Kundeninteraktionen über die entsprechenden Plattformen verstärkt, um Marktanteile zu gewinnen und die Kundenbindung zu verbessern. Die weit verbreitete Nutzung von Social Media- und Messaging-Apps in der APJ-Region bietet Cyberkriminellen zusätzliche Vektoren, um Phishing- und Imitationsangriffe durchzuführen. Häufig wird dabei das Vertrauen missbraucht, das Menschen in diese Plattformen setzen.



Weiterentwicklung der Compliance: Wie globale Cybersicherheitsvorschriften Finanzinstitute prägen

Auf die Frage, warum er Banken ausgeraubt habe, antwortete der berüchtigte Bankräuber Willie Sutton: „Weil dort das Geld ist." Die Aussage von Sutton gilt natürlich auch für aktuelle Cyberangriffe auf Finanzinstitute. Doch die Motivation durch finanziellen Gewinn ist nur die halbe Wahrheit. Finanzinstitute werden zunehmend von Angreifern ins Visier genommen, die von politischen Themen oder geopolitisch-strategischen Motiven geleitet sind. Diese Beweggründe – kombiniert mit der Tatsache, dass „dort das Geld ist" – schaffen eine äußerst kritische Lage für die Finanzdienstleistungsbranche, den am häufigsten angegriffenen Sektor.

Das sollte uns nicht überraschen. Die Finanzbranche spielt seit jeher eine zentrale Rolle für die Gesellschaft und ist Gegenstand umfangreicher Regulierungen. Während sich die Regulierung von Finanzinstituten in der Vergangenheit auf den Schutz von Verbrauchern bei ihren Geschäften mit Finanzinstituten konzentrierte, versuchen die Regulierungsbehörden heute, die Kriterien für Sicherheit und Resilienz kritischer Infrastrukturen auf Finanzinstitute und -dienstleister anzuwenden. Dieser neuere Trend umfasst nicht nur Anforderungen an die Finanzinstitute selbst, sondern auch an ihre IKT-Lieferanten (Informations- und Kommunikationstechnologie).

Es gibt zahlreiche Beispiele für gesetzliche Vorschriften zu Cybersicherheit und betrieblicher Resilienz. In der Europäischen Union schreibt das Gesetz über die digitale betriebliche Resilienz (DORA) vor, dass Finanzunternehmen und ihre Lieferanten über solide IKT-Risikomanagement-Frameworks verfügen und regelmäßige Tests und Vorfallmeldungen durchführen. In den Vereinigten Staaten hat die Securities and Exchange Commission (SEC) Vorschriften für die Cybersicherheit eingeführt, die öffentliche Unternehmen, einschließlich Finanzinstitute, dazu verpflichten, Cybervorfälle offenzulegen, die

ihre Geschäftstätigkeit erheblich beeinträchtigen könnten. In Australien hat die Australian Prudential Regulation Authority (APRA) Standards für Unternehmen festgelegt. Diese müssen Funktionen für Informationssicherheit implementieren, die der Größe und dem Ausmaß der Bedrohungen für ihre Informationsbestände angemessen sind (Verordnung CPS 234). Diese Beispiele veranschaulichen den globalen Trend hin zur Verbesserung der Cybersicherheit und der betrieblichen Resilienz im Finanzsektor. Ziel ist es, den Schutz vor neuen Risiken zu gewährleisten und die Finanzstabilität zu sichern.

Angesichts dieser Vorschriften obliegt es den Finanzinstituten, beim Kauf von IKT- und Sicherheitsservices eine Due-Diligence-Prüfung durchzuführen, um sicherzustellen, dass die Lieferanten diese neuen, strengen Standards erfüllen. Sie sollten sich für Lieferanten entscheiden, die nicht nur einen resilienten Service bieten, sondern auch die relevanten Vorschriften kennen. Die Lieferanten müssen die geforderte Transparenz bieten, damit dynamische Bedrohungen erkannt und abgewehrt werden können, und sie müssen zur Anwendung der Erkenntnisse auf den laufenden Betrieb beitragen.

Transparenz ist von entscheidender Bedeutung, denn Sie können nur Ressourcen schützen, die Sie kennen (und bei denen Sie wissen, womit sie verbunden sind). Und ebenso können Sie sich nicht vor einer Bedrohung schützen, von der Sie gar nicht wissen, dass es sie gibt. Services wie die Akamai Guardicore Platform bieten nicht nur Schutz vor Angriffen, sondern helfen Kunden auch, Datenflüsse zu verstehen, Anomalien zu erkennen und Netzwerkressourcen ordnungsgemäß zu segmentieren, um Bedrohungen abzuwehren. In ähnlicher Weise sind die zugehörigen API-Sicherheitsservices darauf ausgelegt, API-Traffic zu identifizieren, um Unterstützung bei Schatten-APIs zu bieten und potenzielle Angriffe über APIs zu erkennen.

Vielleicht sollten Banken den traditionellen CIA-Ansatz (Confidentiality, Integrity, Availability: Vertraulichkeit, Integrität, Verfügbarkeit) zu VCIA ändern – das V steht hierbei für Visibility, also Transparenz.

James Casey
Vice President, Chief Privacy Officer,
Akamai

Mit Zero Trust zu einer starken Abwehr

Vertrauen bildet die Grundlage, auf der Finanzinstitute ihren Ruf aufbauen. Wenn es jedoch um den Schutz komplexer Umgebungen und vertraulicher Daten geht, kann Vertrauen leicht zu einem Risiko werden. Cyberkriminelle nutzen implizites Vertrauen auf vielfältige Weise aus. Hier sind einige Beispiele:

- Phishing-Angriffe, in denen sie sich als Personen innerhalb des Unternehmens ausgeben
- Angreifer nutzen Sicherheitslücken bei Drittanbietern aus, um Zugang zu hochwertigen Zielen zu erhalten
- Insiderbedrohungen, bei denen der Zugriff für böswillige Zwecke missbraucht wird

Angesichts der zunehmenden Komplexität von Angriffen reicht herkömmliche Netzwerksicherheit nicht mehr aus, da hierbei der gesamte Traffic, der von innen kommt, als vertrauenswürdig eingestuft wird. Aufgrund des hohen Risikos bei Finanzdienstleistungen ist die Aufrechterhaltung einer resilienten Sicherheit von entscheidender Bedeutung. Hier ist das Zero-Trust-Framework zwingend erforderlich. Dieser Sicherheitsansatz basiert auf dem Prinzip, dass jede Verbindungsanfrage, jeder Nutzer oder jedes Gerät eine potenzielle Gefahr darstellt. Er implementiert eine kontinuierliche Überprüfung und entfernt implizites Vertrauen. So wird der Zugriff auf Ressourcen standardmäßig verweigert, es sei denn, der Anforderer ist authentifiziert und autorisiert.

Zero Trust verbessert die Einhaltung dynamischer gesetzlicher Anforderungen für Finanzinstitute, indem Systeme, die regulierte Daten verarbeiten, geschützt werden. So können Unternehmen Strafen vermeiden, die bei nicht bestandenen Audits fällig würden. Zero Trust stellt zusätzliche Kontrollen für ältere Systeme bereit und bietet präzise Einblicke, um unbefugte Nutzer zu erkennen, die versuchen, auf kritische Anwendungen zuzugreifen.

Das Zero-Trust-Modell schränkt den East-West-Traffic ein, indem der Netzwerkzugriff auf kritische Systeme begrenzt und laterale Netzwerkbewegungen von Bedrohungen wie Ransomware verhindert werden. Diese Eindämmungsstrategie schützt wichtige Daten und Ressourcen durch die Isolierung infizierter Systeme. Da die Zahl der Ransomware-Angriffe auf Finanzdienstleister erheblich zugenommen hat, kann die Bedeutung von Zero Trust für den Schutz sensibler Daten gar nicht hoch genug eingeschätzt werden. Dank seiner präzisen Einblicke hilft Zero Trust Ihnen, Bedrohungen in komplexen Umgebungen zu erkennen und zu neutralisieren. Dies ist entscheidend, wenn man die Ausbreitung von Ransomware verhindern und kritische Assets schützen will.

Ein weiterer Vorteil von Zero Trust ist die Fähigkeit, Datenflüsse zwischen Anwendungen zu schützen, was für die sichere Bereitstellung cloudbasierter Anwendungen unerlässlich ist. Das erleichtert nicht nur die Modernisierung, sondern gewährleistet auch den Schutz vertraulicher Informationen in einer dynamischen Bedrohungslandschaft. So können Finanzinstitute Innovationen vorantreiben, ohne Abstriche bei der Sicherheit machen zu müssen. Die Implementierung eines Zero-Trust-Frameworks verbessert die Sicherheitslage und schützt Unternehmen vor neu entstehenden Bedrohungen.

Segmentierung ist gut. Mikrosegmentierung ist besser.

Segmentierung ist ein Architekturansatz, bei dem ein Netzwerk in kleinere Segmente unterteilt wird, um Performance und Sicherheit zu verbessern. Die Mikrosegmentierung ist eine Sicherheitstechnik, mit der Sie ein Netzwerk bis hin zur individuellen Workload-Ebene logisch in verschiedene Sicherheitssegmente unterteilen können. Sicherheitskontrollen und Servicebereitstellung können dann für jedes einzelne Segment definiert werden.

Mikrosegmentierung bildet auch das Fundament von Zero Trust. In einem kürzlich erschienenen Akamai-Bericht nannten befragte Verantwortliche für Cybersicherheit im Finanzdienstleistungssektor die Förderung von Zero Trust als häufigsten Grund für Segmentierungsprojekte. Fast alle befragten Unternehmen, die überhaupt Segmentierungen vorgenommen haben, implementieren ein Zero-Trust-Sicherheitsframework (99 %) oder haben dies bereits getan. Allerdings haben weniger als die Hälfte (47 %) der Befragten ihr Zero-Trust-Framework so weit abgeschlossen und definiert, dass es als ausgereift gelten kann.

Mikrosegmentierung funktioniert mit vorhandenen Systemen und lässt sich schneller als herkömmliche Methoden wie Firewalls einsetzen. Dieser Ansatz beschleunigt die Reaktion auf Ransomware um bis zu 13 Stunden und vereinfacht die Verwaltung in allen IT-Umgebungen. Außerdem trägt er durch präzise Datenkontrolle zur Erfüllung von Compliance-Anforderungen bei.

Ein Beispiel aus der Praxis zeigt den Effekt moderner Mikrosegmentierung: Bei einem Projekt wurde die Implementierungszeit von zwei Jahren auf sechs Wochen verkürzt – mit nur einem Techniker und 85 % weniger Kosten. Dieser Fall veranschaulicht, wie Unternehmen durch Mikrosegmentierung Zeit und Geld sparen können. IT-Leiter sollten diese Ergebnisse mit ihren aktuellen Sicherheitskosten und Implementierungszeiten vergleichen.

Um ihre Cybersicherheit zu stärken, müssen Finanzinstitute die Implementierung fortschrittlicher Segmentierungsstrategien priorisieren. CISOs sollten bei der Anpassung von Sicherheitsmaßnahmen an neue Industriestandards vorangehen und Mikrosegmentierung als Eckpfeiler einer robusten Zero-Trust-Architektur integrieren. IT-Leiter müssen regelmäßig Sicherheitsprüfungen durchführen und Strategien aktualisieren, um sicherzustellen, dass ihre Abwehrmechanismen ausgeklügelten Cyberbedrohungen dauerhaft standhalten können.

Dieser proaktive Ansatz minimiert nicht nur aktuelle Sicherheitsrisiken, sondern versetzt Unternehmen auch in die Lage, neue Herausforderungen im Bereich der Cybersicherheit effektiv zu meistern. Durch Umsetzung dieser Maßnahmen schaffen Finanzinstitute ein umfassendes Sicherheitsframework, das sowohl unmittelbare Sicherheitsprobleme als auch das langfristige Risikomanagement abdeckt.

[Mikrosegmentierung] minimiert nicht nur aktuelle Sicherheitsrisiken, sondern versetzt Unternehmen auch in die Lage, neue Herausforderungen im Bereich der Cybersicherheit effektiv zu meistern.

Abwehr

Wenn es darum geht, Ihr Finanzinstitut vor verschiedenen Cyberbedrohungen zu schützen, müssen Sie einen vielseitigen Ansatz implementieren. Sehen wir uns die wichtigsten Strategien zur Abwehr von Phishing, Markenimitation, DDoS-Angriffen und Ransomware an.

Schutz vor Phishing und Markenimitation

Um Ihr Unternehmen vor Phishing und Markenimitation zu schützen, sollten Sie Markenschutz-Services von Drittanbietern in Erwägung ziehen, um betrügerische Inhalte schnell zu erkennen und zu beseitigen. Außerdem ist es wichtig, Ihre Mitarbeiter und Kunden zu schulen. Führen Sie regelmäßige Sicherheitsschulungen für Ihre Mitarbeiter durch, damit sie sensibilisiert werden und lernen, Phishing- und Imitationsversuche zu erkennen. Vermitteln Sie klar und deutlich, woran sie legitime Mitteilungen Ihres Unternehmens erkennen können. Erstellen Sie einen schnellen Reaktionsplan für Imitationsversuche, einschließlich eines Prozesses zur Benachrichtigung von Partnern und Kunden über Imitationsbetrug.

Darüber hinaus müssen die folgenden Schutztechniken implementiert werden:

- Registrieren Sie ähnliche Domainnamen, um Typosquatting zu verhindern, und verwenden Sie Domain-Überwachungsdienste, um Nachahmungsdomains zu erkennen.
- Stärken Sie Authentifizierungsprotokolle durch die Verwendung starker, eindeutiger Passwörter und Passwortmanager, und implementieren Sie eine leistungsstarke Multi-Faktor-Authentifizierung (MFA) für alle Konten und Systeme.
- Stellen Sie E-Mail-Authentifizierungsprotokolle wie Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) und Domain-Based Message Authentication, Reporting and Conformance (DMARC) bereit, um E-Mail-Spoofing zu verhindern. Verwenden Sie Anti-Phishing-Lösungen und erweiterte E-Mail-Filter, um schädliche E-Mails zu erkennen und zu blockieren.
- Schützen Sie Ihre Website und Ihre digitalen Kanäle, indem Sie SSL-Zertifikate beziehen, HTTPS implementieren und Betrugsbekämpfungstools verwenden, um verdächtige Aktivitäten auf Ihrer Website und Ihren mobilen Apps zu erkennen.
- Schützen Sie Kommunikationskanäle, indem Sie sichere Portale bereitstellen und verschlüsseltes Messaging für vertrauliche Korrespondenz implementieren.

DDoS-Schutz

Der Schutz Ihres Finanzinstituts vor DDoS-Angriffen erfordert eine mehrschichtige Verteidigungsstrategie. Implementieren Sie proaktive Strategien, zum Beispiel die Verwendung spezieller Produkte für DDoS-Erkennung, -Abwehr und -Schutz, die Konfiguration von Ratenbegrenzungen oder das Zwischenspeichern von Inhalten in einem CDN (Netzwerk zur Inhaltsbereitstellung). Darüber hinaus sollten Sie sich über Sicherheitsmaßnahmen wie Patchmanagement, Vorfallsreaktionspläne, Abwehrkontrollen für DDoS-anfällige IP-Adressen und kritische Subnetze, Zugriffssteuerungsrichtlinien, Netzwerksegmentierung und Firewalls auf dem Laufenden halten. Implementieren Sie proaktive Strategien wie die Konfiguration von Ratenbegrenzungen, das Zwischenspeichern von Inhalten in einem CDN oder die Verwendung spezieller Produkte für DDoS-Erkennung, -Abwehr und -Schutz.

Um die DNS-Infrastruktur zu schützen, sollten Sie den eingehenden DNS-Traffic kontinuierlich überwachen und analysieren. Außerdem sollten Sie eine hybride Plattform anstelle einer herkömmlichen DNS-Firewall verwenden. Wenn Sie die Taktiken, Techniken und Verfahren der Angreifer verstehen, können Sie sich besser vor DDoS-Angriffen schützen.

Schutz vor Ransomware

Wie an früherer Stelle bereits erwähnt, ist Zero Trust mit Netzwerksegmentierung, insbesondere Mikrosegmentierung, entscheidend, um die Verbreitung von Ransomware in Ihrem Finanzinstitut zu begrenzen. Die Implementierung leistungsstarker Cybersicherheitsmaßnahmen wie dieser wird dazu beitragen, die fortschrittlichen Techniken zu bekämpfen, die Ransomware-Angreifer heute einsetzen. Bleiben Sie außerdem wachsam und nutzen Sie das MITRE ATT&CK-Framework, um Einblicke in die gängigen Taktiken und Techniken von Angreifern zu erhalten, Ihre Playbooks entsprechend anzupassen und die Ransomware-Kill-Chain zu durchbrechen.

Aktualisieren Sie Ihre Abwehrmaßnahmen kontinuierlich und schulen Sie Ihre Mitarbeiter darin, potenzielle Bedrohungen zu erkennen und effektiv zu beantworten. Integrieren Sie starke Netzwerkabwehr, Endpoint-Schutz, E-Mail-Filterung und regelmäßiges Patchmanagement. Richten Sie eine kontinuierliche Überwachung des Netzwerkverkehrs, der Systemprotokolle und des Nutzerverhaltens ein und implementieren Sie Methoden zur Erkennung von Bedrohungen, um Ransomware proaktiv zu identifizieren.

Implementieren Sie regelmäßige und sichere Datensicherungen, einschließlich Air-Gap-Sicherungen, um sicherzustellen, dass wichtige Informationen im Falle eines Ransomware-Angriffs schnell wiederhergestellt werden können. Implementieren Sie MFA für alle Nutzerkonten, um eine zusätzliche Sicherheitsebene hinzuzufügen.

Durch die Implementierung dieser umfassenden Abwehrstrategien ist Ihr Finanzinstitut deutlich besser in der Lage, sich gegen verschiedene Cyberbedrohungen zu schützen, die Betriebskontinuität sicherzustellen, Ihren Ruf zu schützen und das Vertrauen Ihrer Kunden zu wahren.

Fazit

Wenn Ihr Finanzinstitut die digitale Transformation nutzt, um Kundenerlebnis, betriebliche Effizienz und Wettbewerbsposition zu verbessern, werden auch die Herausforderungen in puncto Sicherheit anspruchsvoller. Gleichzeitig wächst der Druck, die immer neuen regulatorischen Anforderungen zu erfüllen. In dieser Ausgabe des SOTI-Berichts haben bekannte und neu entstehende Bedrohungen für die Finanzdienstleistungsbranche untersucht, die eine kontinuierliche Evaluierung und Verbesserung von Sicherheitslösungen erfordern. Da die Bedrohungen immer ausgefeilter werden, ist es entscheidend, ihnen durch Stärkung von Verteidigungsmaßnahmen und Optimierung von Sicherheitsstrategien einen Schritt voraus zu sein.

DDoS-Angriffe auf Finanzinstitute übertreffen mittlerweile die Attacken auf die Gaming-Branche, die lange Zeit als oberstes Ziel angesehen wurde. Dieser alarmierende Trend unterstreicht die steigenden Risiken. Aufgrund von Faktoren wie Hacktivismus und dem geopolitischen Klima sind Finanzdienstleister heute mehr gefährdet denn je. Gleichzeitig sind das Ausmaß und die Schwere des Traffics bemerkenswert, der durch Nachahmungs- und Phishing-Websites im Finanzdienstleistungssektor generiert wird. Ebenso erstaunlich ist die Geschwindigkeit, mit der Angreifer neue Domains generieren können, nachdem die ursprünglichen Websites abgeschaltet wurden. Die Verfolgung dieser Aktivitäten kann für Unternehmen sehr ressourcenintensiv sein. Deshalb brauchen Sicherheitsteams Lösungen, die Takedown-Services, Threat Intelligence und die Erkennung von Imitationen und Phishing über unterschiedliche digitale Kanäle abdecken.

Verbraucher und Regulierungsbehörden sehen die Finanzinstitute oft in der Verantwortung, wenn sie Opfer von Phishing und anderen Betrugsversuchen geworden sind. Das gilt selbst dann, wenn diese Institute keine direkte Schuld trifft. Noch wichtiger ist, dass Phishing und Markenimitation häufig Wegbereiter für noch gefährlichere Angriffe sind. Deshalb ist es entscheidend, den Angriffszyklus frühzeitig zu unterbrechen. Entschlossene Maßnahmen können darüber entscheiden, ob sie morgen aufgrund eines Sicherheitsvorfalls in den Schlagzeilen stehen oder den Ruf Ihres Unternehmens und das Vertrauen Ihrer Kunden schützen.

Angesichts der unablässigen Angriffe auf Finanzdienstleister bleibt der Schutz vertraulicher Informationen zur Verhinderung von Betrug und Missbrauch eine gewaltige Herausforderung. Die Einführung eines Sicherheitsframeworks wie Zero Trust ist unerlässlich, um sich effektiv vor Phishing-Angriffen zu schützen, die auf Mitarbeiter abzielen. Außerdem wird verhindert, dass sich Ransomware innerhalb von Netzwerken ausbreitet und kritische Assets erreicht. Schließlich gewährleistet ein entsprechendes Sicherheitsframework die Einhaltung bestehender und neuer gesetzlicher Vorschriften auf der ganzen Welt.

Dieser Bericht bietet praktisch verwertbare Einblicke in die neuesten Angriffstrends in der Finanzdienstleistungsbranche und ermöglicht es Ihnen, Ihre Abwehrmaßnahmen zu stärken. Wenn Sie wachsam bleiben und die in diesem Bericht beschriebenen Strategien umsetzen, können Sie Ihr Unternehmen und Ihre Kunden besser vor den zunehmenden Bedrohungen schützen.

Bleiben Sie auf dem Laufenden über unsere neuesten Forschungsergebnisse und besuchen Sie unseren Security Research Hub.

Methodik

DDoS (Layer 7)

Diese Daten beschreiben Warnungen auf Anwendungsebene über Traffic, der unsere Web Application Firewall (WAF) durchläuft. Die L7-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.

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.

Sofern nicht anders angegeben, decken die Daten in diesem Bericht den Zeitraum von 18 Monaten vom 1. Januar 2023 bis zum 30. Juni 2024 ab.

Markenimitationsangriffe

Akamai Brand Protector ist eine Lösung zum Schutz vor Markenmissbrauch, die Unternehmen und ihre Kunden vor Imitationsangriffen wie Phishing, gefälschten Websites, gefälschten Social-Media-Konten und betrügerischen Anwendungen schützt. Sie nutzt das globale Edge-Netzwerk von Akamai, das täglich mehr als 900 Terabyte an Daten analysiert, um Bedrohungen zu erkennen, bevor sie sich auf Kunden auswirken. Diese Informationen werden durch Feeds von Partnern erweitert, um einen umfassenden Überblick über potenzielle Bedrohungen auf verschiedenen Online-Plattformen zu erhalten.

Verschiedene Merkmale jeder erkannten verdächtigen Domain werden analysiert. Die jeweils festgestellten Risikograde werden zur Berechnung der Bedrohungsbewertung für die Domain herangezogen. Diese verdächtigen Domains werden überwacht, die zugehörigen Daten werden verfolgt und die betroffenen Kunden werden auf die bösartigen Kampagnen zum Missbrauch der Markenidentität hingewiesen.

Die Daten in diesem Bericht decken erkannte verdächtige Domains in einem Zeitraum von 12 Monaten vom 1. August 2023 bis zum 31. Juli 2024 ab.

Mitwirkende

Forschungsleitung

Mitch Mayne

Redaktion und Text

James Casey
Lance Rhodes
Badette Tribbey

Prüfung und fachliche Expertise

Cheryl Chiodi
Ziv Eli
Reuben Koh
Gal Meiri
Richard Meeus
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 über die Akamai-Lösungen zur Abwehr von Bedrohungen für Finanzdienstleister finden Sie auf unserer **Seite für Finanzdienstleistungen**.