LINK 11

Reblaze

European Cyber Report

Bedrohungen und Trends in Netzwerksicherheit und Webschutz

Inhalt

Vorwort

Liebe Leserinnen und Leser,

nach der Akquisition von Reblaze Technologies, einem renommierten Anbieter von Cloud-nativem Webanwendungs- und API-Schutz (WAAP), wollen wir gemeinsam das Internet zu einem sichereren Ort machen. Die Bedrohungslage ist akuter denn je. Politisch motivierte Hackergruppen nehmen internationale kritische Infrastrukturen ins Visier, Bots werden immer raffinierter und jede kritische Sicherheitslücke ist ein potenzielles Einfallstor für Cyberkriminelle.

Die täglichen Herausforderungen für Unternehmen nehmen zu, umso wichtiger sind eine proaktive Cybersicherheitsstrategie und innovative Abwehrmaßnahmen. Der „European Cyber Report - Bedrohungen und Trends in Netzwerksicherheit und Webschutz“ löst ab sofort den bisherigen DDoS-Report ab. Der vorliegende Report beleuchtet nicht nur die zunehmende Komplexität der Bedrohungslandschaft, sondern zeigt auf, wie KI-basierte und automatisierte Sicherheitslösungen die Cyber-Resilienz steigern können. Neben der fundierten Analyse der im eigenen Link11-Netzwerk registrierten DDoS-Angriffe werden zusätzliche Inhalte aus den Bereichen Web Protection und Web Performance integriert.

Link11 tritt an, um seine Kunden dabei zu unterstützen, ihre kritischen Assets und ihre Marke zu schützen. Statt Cybersecurity als reinen Kostenfaktor zu sehen, geht es vielmehr darum, mit sicheren Umgebungen Innovation und Wachstum zu ermöglichen und damit schlussendlich abstrakte Sicherheitskonzepte in Wettbewerbsvorteile zu transformieren. Es ist wichtig, den bekannten Schwachstellen deutlich mehr Aufmerksamkeit zu schenken und zu effektiven Schutzmaßnahmen zu greifen.

Ich wünsche Ihnen eine spannende Lektüre!

Herzliche Grüße
Jens-Philipp Jung, CEO, Link11 Group

Einleitung und Zusammenfassung

Zum Stand der Dinge – Netzwerksicherheit und Webschutz im Jahr 2023

Zu Beginn des Jahres warnte Sadie Creese, Professorin für Cybersicherheit an der Oxford-Universität, während des World Economic Forum[1] in Davos vor einem bevorstehenden „Cybersturm“. Obwohl sie im Januar 2023 nicht genau prognostizieren konnte, wie stark dieser Sturm ausfallen würde, hat sich ihre Vermutung als sehr zutreffend erwiesen.

Laut dem aktuellen Allianz Risk Barometer[2] gehören Cyberangriffe zu den größten Bedrohungen für Unternehmen weltweit. Fast alle Unternehmen sind inzwischen auf digitale Dienste und Infrastrukturen angewiesen. Mit dem technologischen Fortschritt sind zwar enorm viele Errungenschaften verbunden, gleichzeitig birgt die umfassende Vernetzung große Risiken. Jedes Netzwerk, jede Webseite oder Schnittstelle, die mit dem Internet verbunden ist, bedeutet ein potenzielles Einfallstor für Cyberkriminelle.

Inzwischen gehören Cyberbedrohungen zum Alltag. Während sie früher ein reines IT-Problem waren, müssen sie heute in jeder Unternehmensstrategie berücksichtigt werden. Auch die Aktivitäten, die das Link11 Security Operations Center (LSOC) im Jahr 2023 beobachtete, machen eines ganz deutlich: Die Auswirkungen von Cybervorfällen erfordern eine risikobasierte, ganzheitliche Cybersicherheitsstrategie, um die Geschäftsziele zu unterstützen sowie das Unternehmenswachstum zu erreichen.

Unser diesjähriger Cybersecurity Report zeigt neben den Entwicklungen der DDoS-Attacken im Link11-Netzwerk relevante Sicherheitserkenntnisse in den Bereichen Bot-Management und WAF, auch bekannt unter dem Kategorienamen WAAP (Web-Application and API Protection). Außerdem skizziert der Report das Zusammenspiel zwischen Geschwindigkeit und Sicherheit für Online-Präsenzen mit Blick auf das Content Delivery Network (CDN). Der Report gliedert sich in die Teile Network Security, Web Protection und Web Performance.

Network Security

Ilm Jahr 2023 verzeichnete das Link11-Netzwerk einen drastischen Anstieg von DDoS-Angriffen um über 70 % im Vergleich zum Vorjahr, wobei politisch motivierte Attacken maßgeblich dazu beitrugen. Diese Angriffe zielten weltweit auf bekannte Ziele wie etwa deutsche Bundesländer und Behörden[3], die europäische Investitionsbank[4] sowie Microsoft[5] ab. Besonders gefährdet sind kritische Infrastrukturen, da erfolgreiche Angriffe schwerwiegende gesellschaftliche, wirtschaftliche und politische Folgen haben können.

Zudem zeigen sich bedenkliche Trends in der Angriffscharakteristik: „Turboangriffe“ erreichen in weniger als 20 Sekunden ihre kritische Nutzlast, die Intensität der DDoS-Angriffe steigt. Es deutet darauf hin, dass die Angreifer vermehrt künstliche Intelligenz einsetzen, um ihre Angriffsmethoden zu verfeinern, wie Europol in ihrem Bericht „The Impact of Large Language Models on Law Enforcement“[6] warnt. Darüber hinaus werden im Link11-Netzwerk verstärkt smarter werdende Multi-Vektor-Angriffe mit einem Fokus auf Effizienz und Ressourcenschonung registriert. Die Angriffsdauer hat sich ebenfalls verlängert. Die längste Attacke im Jahr 2023 dauerte fast 75 Stunden, im Vergleich zu 28 Stunden und 15 Minuten im Jahr 2022.

Web Protection

Neben einem umfassenden DDoS-Schutz ist auch das Bot Management zu einer kritischen Notwendigkeit geworden. Unternehmen sind zunehmend mit einer Vielzahl von automatisierten Datenverkehrsarten konfrontiert, von harmlosen bis hin zu bösartigen Bots. Während einige Bots die Effizienz steigern und betriebliche Abläufe automatisieren, stellen „Bad Bots“ etwa durch die Verbreitung von Spam und Credential Stuffing eine ernsthafte Bedrohung dar. Die fortschreitende Entwicklung von generativer KI und die zunehmende Raffinesse der Angriffe machen einen wirksamen Schutz unerlässlich, während viele Unternehmen immer noch für simple Bot-Attacken anfällig sind.

Es werden verschiedene Techniken eingesetzt, um menschlichen Datenverkehr von maschinell erzeugtem Traffic zu unterscheiden. Angesichts der rapiden Zunahme von Bot-Angriffen und deren schwerwiegenden Auswirkungen auf Unternehmen ist eine differenzierte Herangehensweise erforderlich, die neben technischen Lösungen auch auf ein erhöhtes Sicherheitsbewusstsein der Mitarbeitenden und eine kontinuierliche Anpassung an neue Bedrohungen setzt.

Die steigende Anzahl von Sicherheitslücken und die fortschreitende Komplexität von Web-Applikationen haben die Bedeutung einer zuverlässigen Sicherheitslösung wie der Web-Application Firewall (WAF) hervorgehoben. Angesichts eines alarmierenden Anstiegs von 15 % bei den gemeldeten Sicherheitslücken im Jahr 2023 wird deutlich, dass herkömmliche Firewalls oft nicht ausreichen, um vor immer ausgefeilteren Angriffen zu schützen. Die WAF bietet eine Lösung, indem sie den Datenverkehr auf Anwendungsebene überwacht, verdächtige Aktivitäten erkennt und potenzielle Angriffe wie SQL-Injection, Cross-Site Scripting und Remote Code Execution abwehrt.

WAFs tragen durch die Erkennung und Blockierung verdächtiger Aktivitäten dazu bei, die Sicherheit und Integrität von Webanwendungen zu gewährleisten. Um ihre Wirksamkeit zu maximieren, müssen WAFs jedoch ordnungsgemäß konfiguriert, regelmäßig aktualisiert und durch klare Sicherheitsrichtlinien sowie regelmäßige Überprüfungen unterstützt werden.

Web Performance

Content Delivery Networks (CDNs) bieten durch die weltweite Verteilung von Inhalten Leistungsverbesserungen für die Bereitstellung von Webinhalten. Durch ein redundantes Netzwerk und die nahtlose Integration von Sicherheitsfunktionen gewährleistet das CDN von Link11 eine kontinuierliche Verfügbarkeit der Inhalte und eine zusätzliche Sicherheitsebene für die Infrastruktur. Darüber hinaus sollte bei der Anbieterauswahl auf dessen Einhaltung und Gewährleistung von europäischen Datenschutzbestimmungen geachtet werden.

”

„Die Notwendigkeit eines proaktiven Ansatzes und innovativer Abwehrstrategien wird angesichts der aktuellen Entwicklungen immer drängender. Mit der Implementierung von KI-basierten und automatisierten Sicherheitslösungen können Unternehmen der wachsenden Bedrohung wirksam begegnen. Unternehmen sollten IT-Sicherheitslösungen als Wettbewerbsvorteil betrachten und auf Lösungen setzen, die einfach zu implementieren und zu betreiben sind.“

Karsten Desler, CTO, Link11 Group

Network Security

DDoS in den Nachrichten

Januar 2023

Hacker greifen dänische Zentralbank und Finanzdienstleister an

Die Websites der dänischen Zentralbank und von Bankdata, einem Unternehmen, das IT-Lösungen für die Finanzbranche entwickelt, wurden von DDoS-Angriffen getroffen.[7]

Februar 2023

Mehrere deutsche Flughäfen von DDoS-Angriffen betroffen

Die Websites von sieben deutschen Flughäfen wurden von DDoS-Attacken getroffen und waren nicht erreichbar.[8]

März 2023

Netzwerkangriff auf IT-Dienstleister der Energieversorgung Filstal

Die Energieversorgung Filstal (EVF) ist von einer DDoS-Attacke auf deren IT-Dienstleister imos betroffen, die die Website-Performance deutlich einschränkt.[9]

April 2023

Europäische Flugsicherung: DDoS-Angriff prorussischer Hacker

Die europäische Flugsicherung ist von einem DDoS-Angriff getroffen worden, für den prorussische Hacker verantwortlich gemacht werden.[10]

Mai 2023

Hackergruppe „Anonymous Sudan" fordert 3 Millionen Dollar von Scandinavian Airlines

Anonymous Sudan hat eine Lösegeldforderung in Höhe von 3 Millionen Dollar an Scandinavian Airlines (SAS) gestellt, um die DDoS-Attacken zu stoppen.[11]

Juni 2023

DDoS-Angriff auf die Europäische Investitionsbank

Prorussische Hacktivisten haben europäische Bankinstitute angegriffen und die Europäische Investitionsbank (EIB) als eines ihrer Opfer genannt.[12]

Juli 2023

DDoS-Angriff auf norwegische Regierungswebseiten

Auf 12 seiner Websites kam es aufgrund einer Software-Schwachstelle bei einem Technologie-dienstleister zu DDoS-Attacken.[13]

August 2023

Mehrere italienische Bankwebseiten lahmgelegt

Italiens Cybersicherheitsbehörde hat Hackerangriffe auf die Websites von mindestens fünf Banken festgestellt, die den Zugang zu einigen ihrer Dienste vorübergehend unmöglich machten.[14]

September 2023

Online-Banking von Wells Fargo außer Betrieb

Anonymous Sudan hat das US-amerikanische Finanzdienstleistungsunternehmen Wells Fargo lahmgelegt und das Online-Banking deaktiviert.[15]

Oktober 2023

Gastgeber des EU-Gipfels Spanien Ziel von DDoS-Cyberangriffen

Mehrere öffentliche und private Websites, sind Ziel eines DDoS-Angriffs prorussischer Hacker geworden.[16]

November 2023

DDoS-Angriff für ChatGPT-Ausfall verantwortlich

OpenAI hat bestätigt, dass eine DDoS-Attacke für die Ausfälle von ChatGPT und dessen Entwickler-Tools verantwortlich ist.[17]

Dezember 2023

DDoS-Attacken auf mehrere belgische Websites

Aufgrund eines DDoS-Angriffs sind mehrere Websites belgische Regierungsstellen ausgefallen.[18]

Entwicklung der Gesamtzahlen im Link11-Netzwerk

Anzahl der DDoS-Angriffe stark gestiegen

Nachdem im vergangenen Jahr im Link11-Netzwerk erstmals ein Rückgang der DDoS-Angriffe verzeichnet wurde, ist die Anzahl der Attacken im Jahr 2023 wieder deutlich angestiegen. Die Anzahl der DDoS-Angriffe hat im Vergleich zum Vorjahreszeitraum um mehr als 70 % zugenommen. Damit verbunden ist auch die Zunahme der täglichen Attacken.

Neben dem anhaltenden Krieg zwischen Russland und der Ukraine hat der Konflikt in Israel einen weiteren Anstieg politisch motivierter DDoS-Angriffe durch wohlorganisierte Angreifer ausgelöst. Zu den prominenten Akteuren zählen die prorussische Gruppen NoName057(16), Anonymous Sudan und Killnet. Alle haben gemeinsam, dass DDoS-Attacken von ihnen als bevorzugtes Mittel der ideologisch motivierten Cyberangriffe eingesetzt werden.

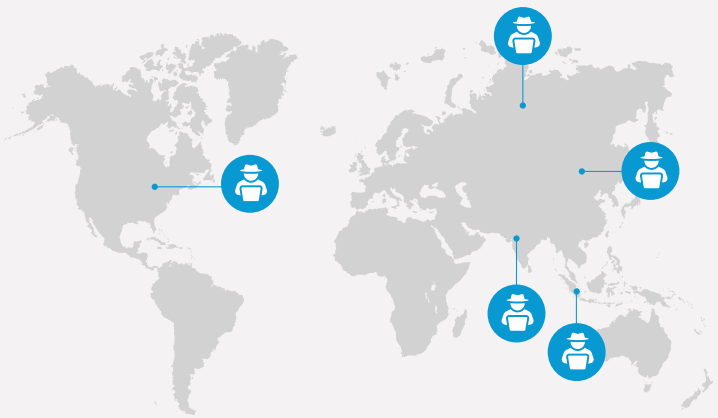
Weltweit nehmen die geopolitischen Spannungen zu, sodass die Bedrohung durch solche Angriffe weiterhin wächst. Viele dieser DDoS-Attacken zielen auf kritische Infrastrukturen (KRITIS), öffentliche Einrichtungen und politische Organisationen ab. Es ist kaum ein Monat vergangen, ohne dass es zu Cyberangriffen auf NATO-Staaten und deren kritische Infrastrukturen kam. Die neue BSI-Chefin Claudia Plattner warnte Anfang Juli 2023, dass die Bedrohungslage so groß wie nie sei.[19]

Über das ganze Jahr haben die DDoS-Aktivitäten im Rahmen des patriotischen Hacktivismus im Vergleich zum Vorjahr weiter zugenommen. Mit der Einführung des „DDoSia-Projekts“, eines speziellen DDoS-Toolkits, haben nicht nur die Möglichkeiten der Angreifer zugenommen, sondern auch die Anzahl der Attacken. Das bereits 2022 gelaunchte Projekt wird seitdem von NoName057(16) und deren Unterstützern weiterentwickelt. Durch ein solches Tool wächst das Bedrohungspotenzial politisch motivierter Cyberangriffe kontinuierlich und gefährdet Sektoren wie Energie, Finanzen und Gesundheitswesen.

Diese Bereiche sind besonders anfällig für DDoS-Angriffe, die nicht nur finanziellen Schaden in Millionenhöhe verursachen, sondern auch zu gefährlichen Versorgungsengpässen führen und sogar Menschenleben gefährden können. Ein Blick auf die geographische Verteilung zeigt, dass die Attacken weltweit Organisationen, Unternehmen und die kritische Infrastruktur in Mitleidenschaft ziehen.

Besonders viel bösartiger Datenverkehr stammte aus den USA, Russland und China. Dicht gefolgt von Indonesien und Indien. Gleichzeitig sind bei einem DDoS-Angriff immer mehrere Länder involviert. Neben den genannten Nationen konnte auch in Deutschland, Großbritannien, Thailand und Italien verstärkt schädlicher Traffic beobachtet werden.

Herkunftsländer der im Link11-Netzwerk registrierten DDoS-Angriffe



DDoS-Angriffe sind längst kein bloßes Ärgernis mehr, sondern eine reale Gefahr für Unternehmen und Institutionen weltweit. Sie sind zu einem wirksamen Mittel geworden, um politische Absichten voranzutreiben und kritische Infrastrukturen zu gefährden. Ein proaktiver Ansatz und innovative Abwehrstrategien sind unerlässlich, um dieser Bedrohung effektiv zu begegnen und unsere Gesellschaft vor schwerwiegenden Konsequenzen zu schützen. Mehr dazu finden Sie im Link11-Whitepaper: *Kritische Infrastrukturen im Fadenkreuz.*

„Die Bedrohungslage ist akuter denn je. Angesichts begrenzter Ressourcen wie Budgets und Fachkräfte sollten Unternehmen auf IT-Sicherheitslösungen setzen, die einfach zu implementieren und dennoch zuverlässig zu betreiben sind. KI-basierte und automatisierte Sicherheitslösungen gewährleisten effektiven Schutz."

Rolf Gierhard, CRO, Link11

NoName057(16) – Hacktivismus 2.0 und das DDoS-Angriffstool „DDoSia"

Im langanhaltenden Konflikt zwischen Russland und der Ukraine hat NoName057(16) als prorussische Hacktivistengruppe besondere Aufmerksamkeit erregt. Seit März 2022 ist die Gruppe aktiv und führt politisch motivierte Distributed-Denial-of-Service Angriffe (DDoS) auf europäische Nationen und deren kritische Infrastrukturen aus. Mit einer Erfolgsquote von 40 Prozent hat NoName057(16) mehr als 5.000 Angriffe[20] durchgeführt, wobei Regierungseinrichtungen, der Verkehrs- und Finanzsektor zu den Hauptzielen zählten.

Die Gruppe hat sich von einer scheinbar unbedeutenden Einheit zu einem gut organisierten Kollektiv mit einer starken Online-Community entwickelt. Mit mehr als 60.000 Abonnenten auf ihrem Telegram-Kanal setzt die Gruppe auf eine innovative Herangehensweise mit dem Crowdsourcing-Botnet-Projekt „DDoSia"[21], dem Nachfolger des Bobik DDoS-Botnets.[22]

Dabei vereint NoName057(16) ideologische Motive mit finanziellen Anreizen für Mitglieder und Unterstützer. Die „heroes" können sich mit ihrer ID-Nummer und einer Krypto-Wallet beim Telegram-Bot registrieren und profitieren von Kryptozahlungen in Höhe von 20.000 (200€) bis 80.000 (800€) Rubel, je nachdem, wie groß ihre eigenen Angriffe im Verhältnis zur Anzahl aller DDoS-Attacken für einen bestimmten Zeitraum waren[23]. Obwohl die Hackergruppe täglich mindestens einen DDoS-Angriff durchführt, der sich an globalen Ereignissen oder am aktuellen Nachrichtenzyklus orientiert, gehören inzwischen auch Desinformations- und Einschüchterungskampagnen zum Repertoire. Die professionell aufgestellte Gruppe unterhält sogar einen eigenen Support-Channel in Englisch.

DDoSia ist das Toolkit, das speziell von NoName057(16) für DDoS-Angriffe entwickelt wurde. Es besteht aus Command & Control Servern und DDoSia-Clients, die es Freiwilligen ermöglichen, ihre Computer und Internetanschlüsse für Angriffe zur Verfügung zu stellen. Die Angriffe werden via Telegram organisiert. Damit werden Ziele gebündelt und maximaler Schaden angerichtet.

Ursprünglich in Python geschrieben, wechselten die Hacker auf Go, um die Effizienz zu verbessern. Die Kommunikation zwischen den DDoSia-Clients und den C2-Servern ist personalisiert und verwendet User-Hashes zur Identifikation der Teilnehmenden. Die Angriffsziele werden von den C2-Servern empfangen und das Tool generiert entsprechende Anfragen. Wie bei DDoS-Attacken üblich, wird legitimer Datenverkehr imitiert, um automatisierte Erkennungssysteme zu umgehen. Diese Technologie erschwert die automatische Erkennung und Blockierung schädlicher Anfragen erheblich.

Angesichts der ständigen Weiterentwicklung und des Wachstums der DDoSia-Community ist sicher: Das Angriffstool „DDoSia" ist in der Cyberwelt angekommen und wird so schnell nicht mehr verschwinden. Schutzlösungen, die in ein umfassendes Sicherheitskonzept integriert sind, sind daher entscheidend, um sich vor solchen Angriffen effektiv zu schützen.

Entwicklung des „Onsets“

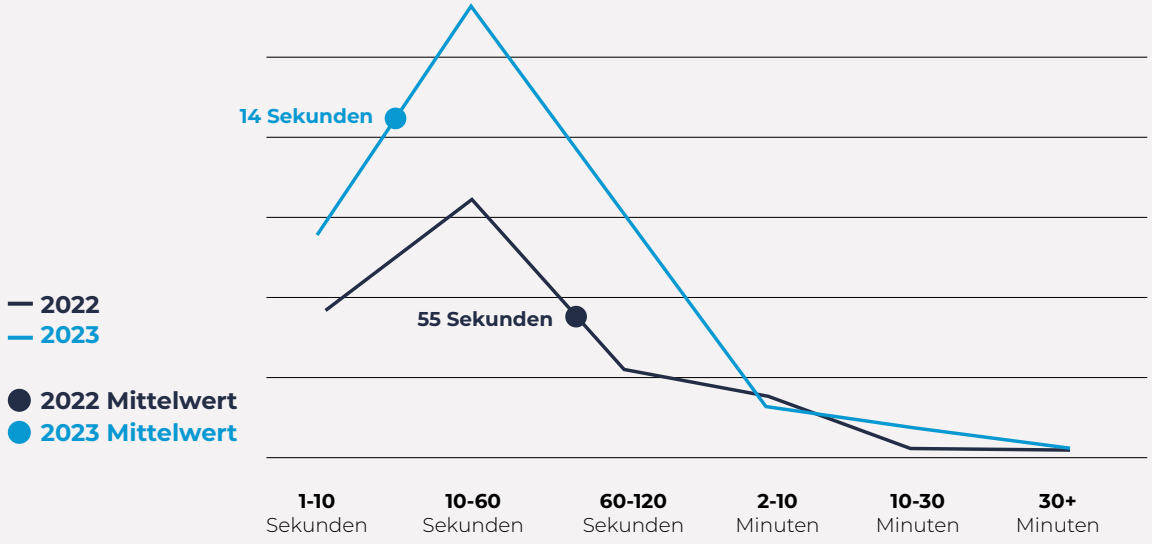
Smarte Turboattacken auf dem Vormarsch

Bei den im Link11-Netzwerk registrierten DDoS-Attacken wird seit dem ersten Halbjahr 2022 zudem ermittelt, wie viele Sekunden nach der Übertragung der ersten Bytes vergehen, bis der Traffic seinen Maximalwert erreicht. Diese DDoS-Angriffe sind anders: Sie kündigen sich nicht mit einer langsamen Steigerung des Angriffes an, sondern erreichen in kürzester Zeit ihre kritische Nutzlast.

Dadurch können Netzwerksysteme bereits lahmgelegt werden, bevor die Abwehrmaßnahmen wirken. Das LSOC spricht bei diesem Angriffszeitraum von „Onset“. Dabei steht die Zeitspanne im Fokus, die ein Angriff braucht, um ein besonders schlagkräftiges Volumen zu erreichen.

Im Jahr 2023 erreichten DDoS-Angriffe im Durchschnitt bereits nach 14 Sekunden ein kritisches Niveau. Verglichen mit dem Durchschnitt von 55 Sekunden im Vergleichszeitraum 2022 erzielten diese „Turboangriffe“ bedeutend schneller ein kritisches Volumen.

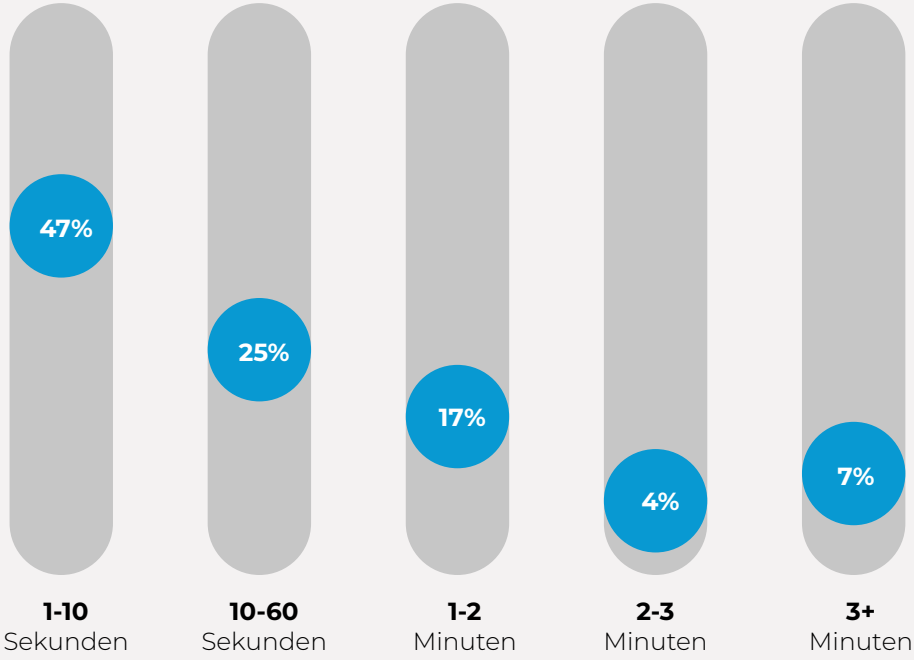
Dauer bis zum Höhepunkt einer Attacke I 2023 vs. 2022



„Normalerweise haben Angriffe eine Anlaufzeit, bevor sie ihr kritisches Potenzial erreichen. Der Onset ist ein wichtiger Faktor bei der Bewertung von DDoS-Angriffen. Dabei wird bemessen, wie schnell ein Angriff sein kritisches Volumen erreicht. Je eher die kritische Nutzlast erreicht ist, desto professioneller und koordinierter war der Angriff.“

Sean Power, Solution Engineer, Link11

Verteilung der Dauer bis zum Höhepunkt der Attacke



Ein Blick auf die Verteilung der Zeit, die während des DDoS-Angriffes bis zum Erreichen des Höhepunktes vergeht, zeigt für den Betrachtungszeitraum folgende Ergebnisse: In knapp der Hälfte der Angriffe (47 %) wurde innerhalb der ersten zehn Sekunden die kritische Nutzlast erreicht. Im Jahr 2022 lag dieser Anteil bei einem Viertel (28 %).

Im Jahr 2023 machten Angriffe, die in 10 bis 60 Sekunden ihren Maximalwert erzielten, ein Viertel aller im Netzwerk registrierten Attacken aus (25 %). Im Vergleich dazu näherten sich fast die Hälfte der Angriffe (47 %) im Jahr 2022 in der gleichen Zeit ihrem Höhepunkt.

In knapp einem Fünftel der Fälle (17 %) dauerte es bei den DDoS-Angriffen im ersten Halbjahr 2023 zwischen einer und zwei Minuten, bis der kritische Maximalwert erreicht wurde. Dieser Wert lag im Vorjahreszeitraum bei 13 %.

Bei jedem zehnten Angriff (11 %) der vom LSOC verzeichneten DDoS-Attacken dauerte es mehr als zwei Minuten, bis das kritische Niveau erreicht wurde. Im Vergleichszeitraum 2022 erreichten 12 % der Angriffe in mehr als zwei Minuten ihren Höhepunkt.

> **Die Charakteristik solcher „Turboangriffe“ lässt Rückschlüsse darauf zu, dass es sich bei den Angriffen um ein Botnetz mit einer entsprechenden Kapazität gehandelt haben könnte. Nur wenn ausreichend Datenverkehrsvolumen erzeugt wird, wie zum Beispiel beim „DDoSia“-Botnetz, erreichen Angriffe in solch kurzer Zeit ihren kritischen Höhepunkt. Denn anders als bei herkömmlichen Botnetzen handelt es sich bei „DDoSia“ um privat zur Verfügung gestellte Rechenleistung.**

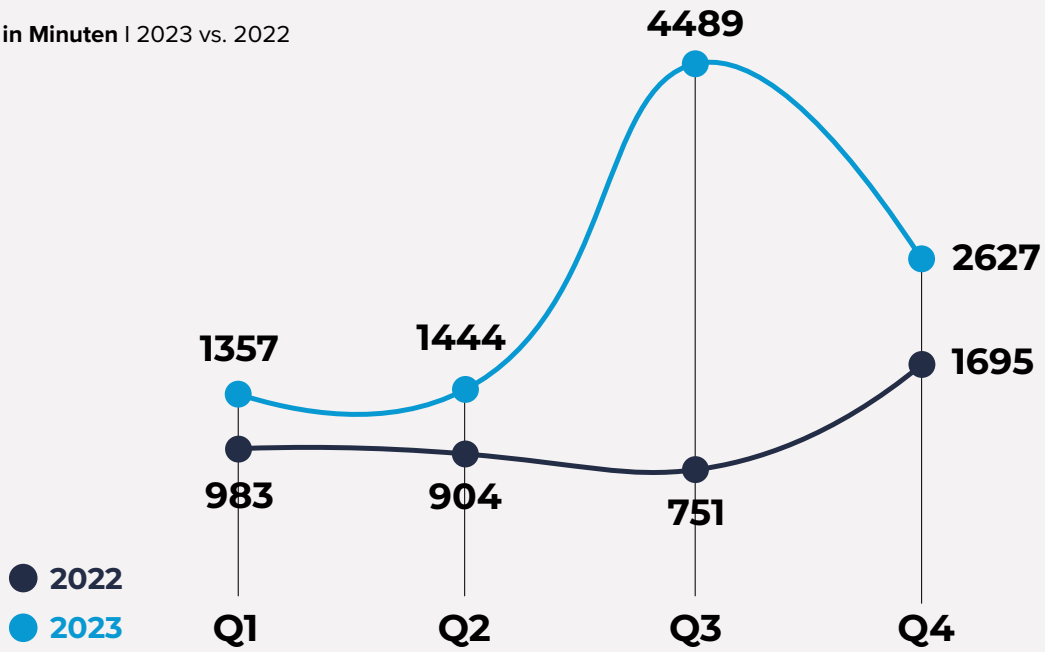
Entwicklung der Angriffsdauer

Angriffe werden länger

Die Dauer, der im Jahr 2023 im Link11-Netzwerk registrierten DDoS-Angriffe, hat sich im Vergleich zum Vorjahr insgesamt verlängert. Ein Blick auf die Grafik unten zeigt deutlich, wie sich die Dauer der DDoS-Attacken 2023 gegenüber 2022 entwickelte.

Insgesamt zeigt sich, dass die jeweils längsten Attacken deutlich voneinander abweichen. Das Jahr 2023 war von insgesamt längeren Attacken geprägt, während im vergangenen Jahr sich ein Trend zu kürzeren DDoS-Angriffen abgezeichnet hatte. Die längste Attacke im Jahr 2023 war 4.489 Minuten lang, das entspricht 74 Stunden und 49 Minuten. Der längste DDoS-Angriff 2022 betrug lediglich 1.695 Minuten, also 28 Stunden und 15 Minuten.

Angriffsdauer in Minuten I 2023 vs. 2022



„Zeit ist ein entscheidender Faktor. Im Angriffsfall kommt es auf jede Sekunde an – überlistete Abwehrmechanismen, Routing-Probleme oder manuelle Bewertungen setzen die IT-Abteilungen zusätzlich unter Druck. Eine Echtzeit-Analyse des Datenverkehrs mit cloudbasierter KI-Technologie ist der Schlüssel, um DDoS-Angriffe blitzschnell abzuwehren und einen Systemausfall zu verhindern."

Jag Bains, VP Solution Engineering, Link11

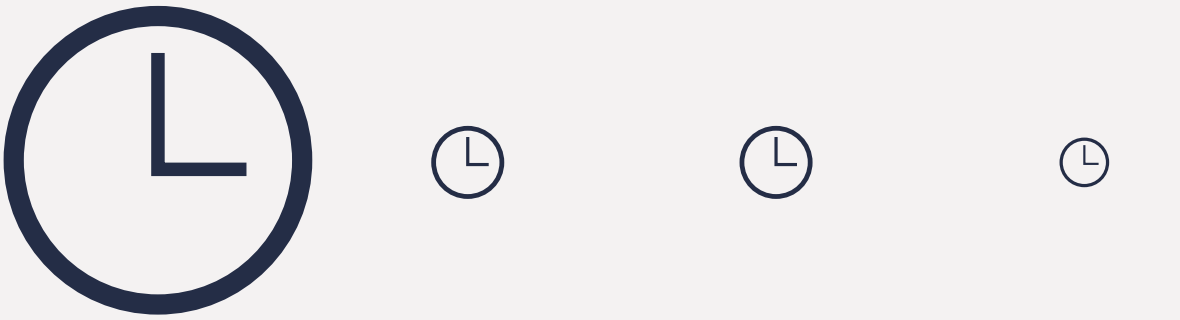
Die weitere Analyse zeigt, dass die Länge der Angriffe zwischen wenigen Minuten und mehreren Stunden schwankte. Die absolute Mehrheit der Angriffe (88 %) dauerte weniger als 5 Minuten. 5 % aller registrierten Angriffe war zwischen 5 und 10 Minuten lang, weitere 5 % bis zu 60 Minuten. 2 % der Angriffe waren länger als 60 Minuten. Verglichen mit dem Vorjahr zeigt sich bei diesen langanhaltenden Angriffen eine Verdopplung.

Die Dauer eines DDoS-Angriffs hängt stark von der angewandten Angriffstechnik ab. Mit Blitzangriffen auf einzelne IP-Adressen versuchen Hacker, oft Schwachstellen in der IT-Infrastruktur ihres Ziels zu identifizieren. Andererseits dienen kleine, schnelle DDoS-Attacken häufig als Tarnung für parallele Hacker-Angriffe auf Server und Netzwerke. Denn hinter diesem DDoS-Vorhang können Hacker unbemerkt durch die Hintertür eindringen.

In solchen Fällen werden vorhandene IT-Ressourcen schnell mobilisiert, um Systemausfälle und Schäden zu minimieren. Kurze Angriffe, die abrupt abgebrochen werden, deuten zudem darauf hin, dass Angreifer ihr Ziel nicht erreichen konnten. Bei gut geschützten Infrastrukturen ziehen sich Angreifer zurück, um Ressourcen zu schonen. Jedoch zielen sie bei langanhaltenden Attacken darauf ab, ihre Ziele dauerhaft zu beeinträchtigen und Schäden zu verursachen.

Die Dauer eines Angriffes allein ist jedoch kein Indikator für die Stärke einer DDoS-Attacke. Ein Angriff kann seinen Höhepunkt erreichen, ohne großen Schaden anzurichten. Ein anderer Angriff kann bereits kritische Auswirkungen wie einen vollständigen Ausfall haben, bevor das maximale Angriffspotenzial ausgeschöpft wird. Gerade bei schnell einsetzenden Angriffen ist die Time-to-Mitigate (TTM) entscheidend. Wie gut Link11 und andere Anbieter in Bezug auf diesen entscheidenden Faktor abschneiden, kann in der Frost & Sullivan-Studie nachgelesen werden: **„The New Benchmark: Why Fast DDoS Detection Is No Longer Good Enough“.**

Verteilung der Angriffsdauer 2023



<5 min	5-10 min	10-60 min	60+ min
88%	5%	5%	2%

Eine effektive IT-Sicherheitsstrategie bedingt eine Echtzeit-Analyse des Datenverkehrs mit smarten, schnellen und sicheren Methoden, um maximale Transparenz im Netzwerk zu gewährleisten. Dabei bildet die Kombination aus einem Basis-Schutz und intelligenter, automatisierter KI-Technologie das Rückgrat der Abwehrmaßnahmen gegen DDoS-Angriffe.

Entwicklung der Angriffsbandbreiten

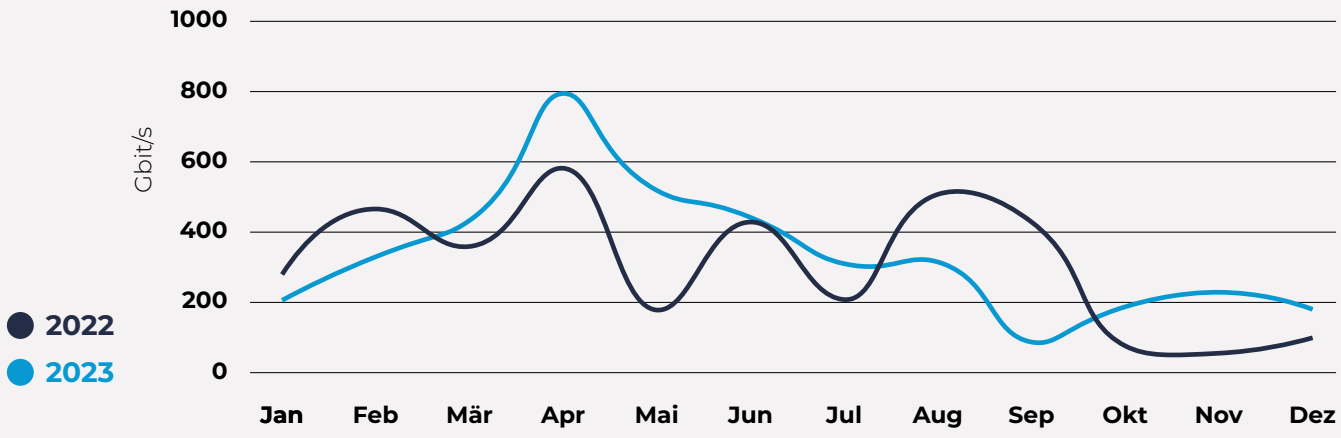
DDoS-Angriffe: Intensiv und komplex

Im Jahr 2023 haben wir mehr Hochvolumen-Attacken gesehen als im Jahr 2022. Während im Jahr 2023 die vom LSOC gemessenen Bandbreiten jeden Monat die Marke von 100 Gbit/s überschritten, zeigt die untenstehende Grafik im Verlauf deutliche Schwankungen für das Jahr 2022. Im Oktober und November 2022 lagen die Bandbreiten-Peaks sogar deutlich unter 100 Gbit/s.

Die größte Attacke im Jahr 2023 wurde bei 795 Gbit/s gestoppt, was im Vergleich zu 2022 eine deutliche Steigerung darstellt. Im ersten Halbjahr schwankten die Bandbreiten der Hochvolumen-Attacken zwischen 261 Gbit/s und dem höchsten gemessenen Einzelausschlag von 795 Gbit/s. Im zweiten Halbjahr nahm die Intensität der Attacken wieder ab. Der größte DDoS-Angriff im dritten und vierten Quartal 2023 wurde bei nur 303 Gbit/s gestoppt.

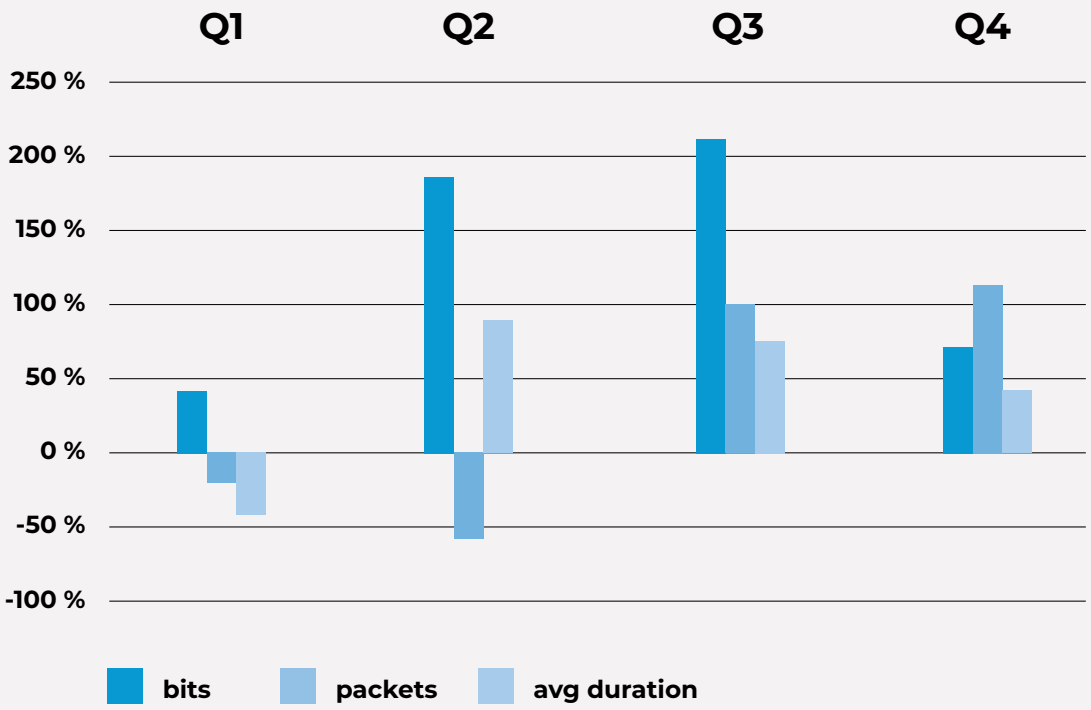
Die durchschnittliche Gesamtbandbreite ist erneut von 2,6 Gbit/s im Jahr 2022 auf 3,0 Gbit/s gestiegen. Die Intensität spiegelt sich nicht nur in der durchschnittlich größeren Bandbreite wider, sondern auch in der Menge an den übertragenen Paketen. Im Betrachtungszeitraum wurde mit mehr als 168 Millionen Paketen pro Sekunde die größte bisher im Link11-Netzwerk registrierte Paketrate beobachtet. Die durchschnittliche Paketrate im Betrachtungszeitraum lag bei 625.000 Paketen pro Sekunde, der Durchschnitt im Jahr 2022 war hingegen deutlich höher. Im Angriffsfall wurden durchschnittlich 3,3 Millionen Pakete pro Sekunde übermittelt.

Bandbreiten-Peak pro Monat | 2023 vs. 2022



Bereits 2022 konnte eine verstärkte Intensität der Angriffe beobachtet werden. Dieser Trend hat sich im Jahr 2023 mit einer weiteren Zunahme der durchschnittlichen Bandbreiten fortgesetzt. Gleichzeitig offenbart ein Blick auf die Korrelation zwischen Dauer und Intensität der DDoS-Angriffe besonders ab dem zweiten Quartal 2023 eine weitere Veränderung: Die intensiveren Angriffe halten länger an.

Veränderung in Dauer und Intensität der Attacken 2023



Website vs. ISP-Killers

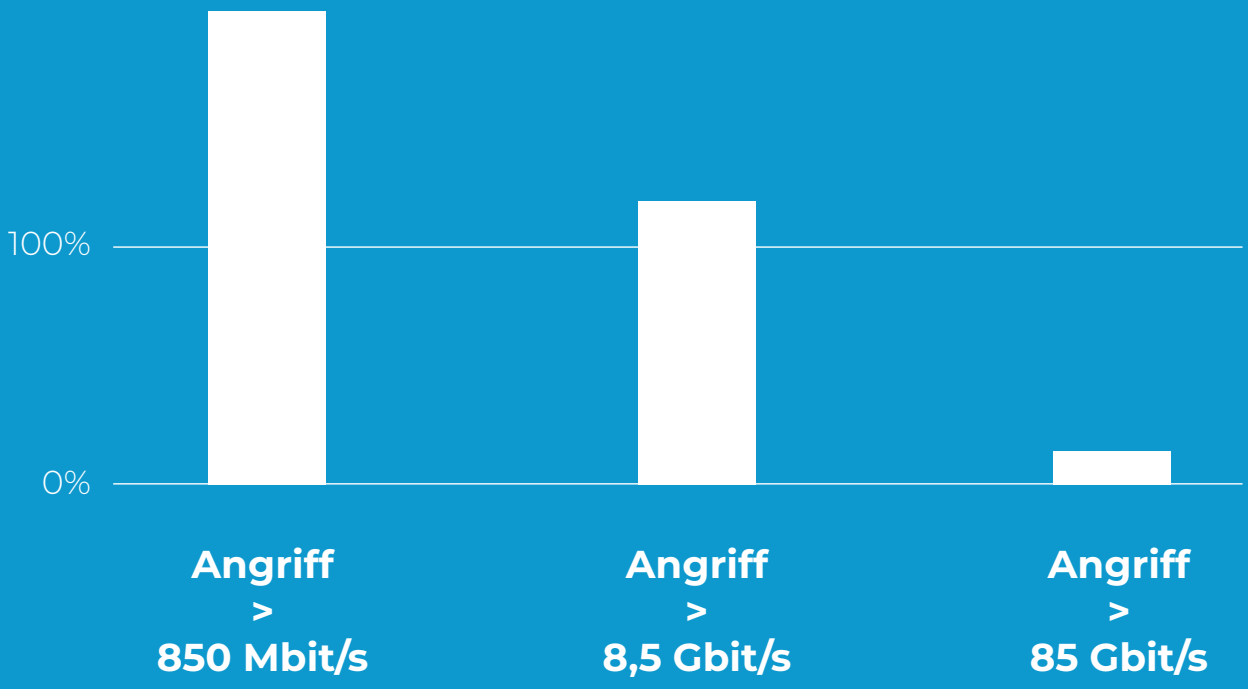
Ein weiterer Blick auf die im Link11-Netzwerk registrierten DDoS-Angriffe zeigt, dass sich die Größenverteilung der Attacken verändert hat. Im Vergleich zum Vorjahr haben Attacken zugenommen, die größer sind entweder als 850 Mbit/s, 8,5 Gbit/s oder 85 Gbit/s. Was bedeutet dies aber nun für Unternehmen?

Viele Unternehmen haben inzwischen eine 10 Gbit/s Uplink-Kapazität. Erreichen Angriffe 85 % der Gesamtkapazität dieser Upstream-Leitung, kann diese überlastet und im schlimmsten Fall komplett lahmgelegt werden. Dazu sind alle Attacken in der Lage, die größer sind als 8,5 Gbit/s. Das Gleiche gilt mit den weniger häufigen 100 Gbit/s Uplink-Kapazitäten großer Internet-Service-Provider (ISP). Ein mehr als 85 Gbit/s großer DDoS-Angriff hat das Potenzial, auch einen ISP bzw. dessen Upstream-Leitung vollständig zu überlasten.

Gleichzeitig konnte auch eine Zunahme kleinerer Attacken beobachtet werden. Die Anzahl derjenigen Angriffe ist gestiegen, die größer sind als 850 Mbit/s. Das lässt Rückschlüsse darauf zu, dass die Intelligenz der DDoS-Attacken größer wird. Diese smarteren Attacken erreichen weder für eine 10 Gbit/s noch für eine 100 Gbit/s große Upstream-Leitung ein kritisches Niveau. Stattdessen können mit Attacken dieser Größe bereits Websites lahmgelegt werden.

Eine robuste IT-Sicherheitsstrategie erfordert eine kontinuierliche Echtzeit-Analyse des Datenverkehrs, um eine maximale Transparenz im Netzwerk zu gewährleisten. Eine erfolgversprechende Abwehr von DDoS-Angriffen besteht aus einem Basis-Schutz und einer Kombination aus intelligenter und automatisierter KI-Technologie. Angesichts der wachsenden Komplexität und Intensität von Angriffen ist es entscheidend, auf Präzision und Schnelligkeit bei der Erkennung und Abwehr zu setzen. Die Zeitfenster für eine effektive Reaktion auf solche Angriffe sind oft sehr knapp. Umso wichtiger ist es, die implementierten Abwehrmaßnahmen kontinuierlich zu überprüfen und zu optimieren.

Veränderung der Größenverteilung der DDoS-Angriffe I 2023 vs. 2022



Multi-Vektor-Attacken

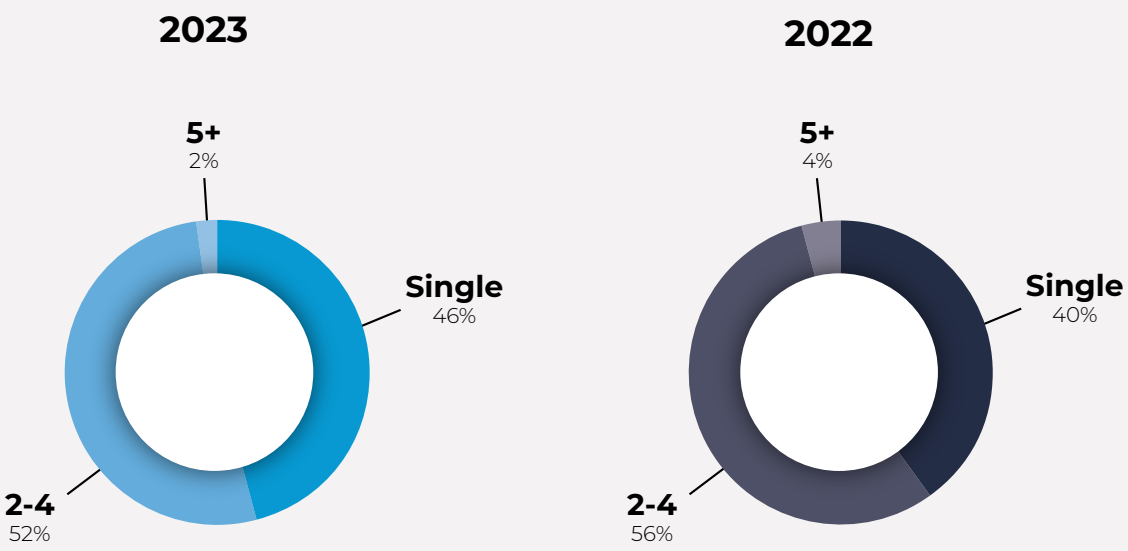
Multi-Vektor-Attacken: smarter und effizienter

Multi-Vektor-Attacken zeichnen sich durch ihre Vielschichtigkeit aus. Im Gegensatz zu herkömmlichen Angriffen, bei denen nur ein Angriffsvektor genutzt wird, richten sich Multi-Vektor-Angriffe parallel an mehrere Schwachstellen in den Bereichen Transport, Applikation und Protokoll. Diese Kombination erschwert die Erkennung und Abwehr der Angriffe erheblich, da die Verteidigungssysteme mit mehreren Angriffsvektoren konfrontiert sind.

Diese Angriffe sind besonders gefährlich, da sie die Erfolgswahrscheinlichkeit für die Angreifer steigern. Beim Einsatz verschiedener Vektoren erhöht sich die Wahrscheinlichkeit, dass zumindest einer der Vektoren erfolgreich ist und die Verteidigungsmaßnahmen durchbricht. Hinkt die IT-Sicherheit der Bedrohungslandschaft hinterher, genügt bereits ein einzelner Vektor, der gezielt und konzentriert eingesetzt wird, um großen Schaden anzurichten.

Im Jahr 2023 hat der Anteil der Multi-Vektor-Angriffe im Vergleich zum Vorjahr leicht abgenommen. Der Anteil von Multi-Vektor-Attacken lag im Jahr 2023 bei 52 %, während wir 56% multidimensionale Angriffe im Jahr 2022 messen konnten.

Anzahl der Single- und Multi-Vektor-Angriffe I 2023 vs. 2022



Unternehmen sollten im Hinblick auf Multi-Vektor-Attacken auf eine umfassende IT-Sicherheitsstrategie setzen. Dazu gehören spezialisierte DDoS-Schutzlösungen, die effektiv gegen verschiedene Angriffsvektoren auf allen Filterebenen arbeiten können. Ein solches System kann Angriffe in Echtzeit erkennen und abwehren, um das Risiko einer längeren Downtime zu minimieren. Zudem ist es wichtig, die Sicherheitsinfrastruktur regelmäßig zu aktualisieren und auf dem neuesten Stand zu halten.

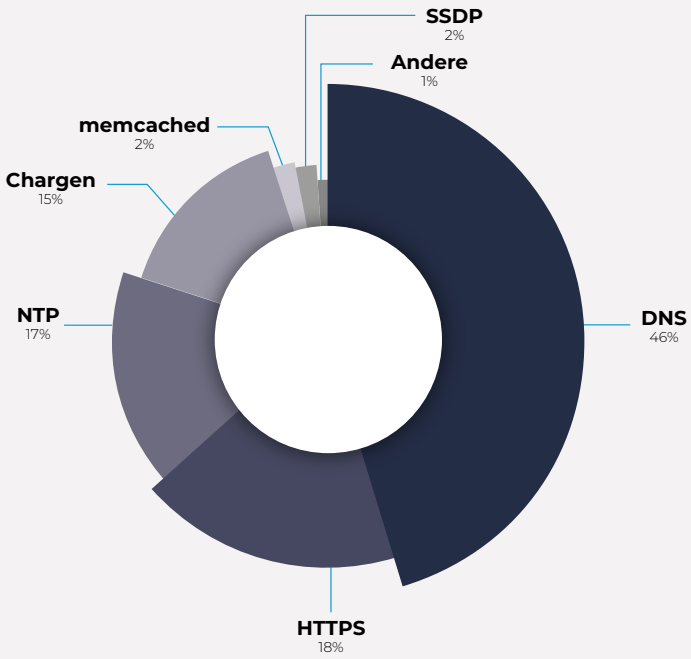
Die höchste Anzahl an im Link11-Netzwerk beobachteten gleichzeitig eingesetzten Vektoren betrug 11. Im Jahr 2022 betrug die Anzahl gleichzeitig eingesetzter Vektoren 18. Dies waren bisher die von unseren beobachteten Multi-Vektor-Attacken die größten im Netzwerk.

Statt wahllos mit vielen verschiedenen Vektoren anzugreifen, kommen solche Vektoren gezielt zum Einsatz, die den meisten Erfolg versprechen. Die Anzahl kommt daher mehr und mehr in die „Mitte“, d. h. es werden überwiegend zwischen zwei und vier Vektoren eingesetzt. Das lässt Rückschlüsse darauf zu, dass die DDoS-Attacken smarter und ressourcenschonender werden.

Durch die gleichzeitige Ausnutzung der identifizierten Schwachstellen können Angreifer ihre Attacken vielschichtiger gestalten und gezieltere Schäden verursachen. Daher ist es für Unternehmen unerlässlich, ihre DDoS-Abwehrstrategien zu optimieren und robuste Sicherheitslösungen einzusetzen, die in der Lage sind, Multi-Vektor-Angriffe zu erkennen, zu analysieren und wirkungsvoll zu neutralisieren.

In fast der Hälfte (46 %) der Multi-Vektor-Attacken ist DNS als Vektor eingesetzt worden, in knapp einem Fünftel (18 %) nutzten die Angreifer HTTPS oder NTP (17 %).

Angriffsvektoren 2023



„Die Bedrohungslandschaft ist in einem permanenten Wandel. Auch wenn der Einsatz weniger Vektoren nach einer Verschnaufpause aussieht, ist die Gefahr nicht gebannt – die Effizienz der DDoS-Angriffe wird größer. Sie werden immer vielfältiger und smarter.“

Jens-Philipp Jung, CEO, Link11 Group

Reflection-Amplification-Angriffe

Angriffsbasis sind fundamentale Internetsysteme

Reflection-Amplification-Attacken sind bösartige Multi-Vektor-Angriffe, die sich auf das Ausnutzen falsch konfigurierter Server und Services im Internet verlassen. Bei einem Reflection-Angriff tarnt der Angreifer die IP-Adresse des Ziels (auch als Spoofing bekannt) und sendet Informationsanfragen über Dienste wie DNS oder NTP. Es gibt viele solcher Internetdienste, bei denen die Verifizierung des Absenders nicht unterstützt wird oder erforderlich ist.

Die Angreifer senden kleine Datenmengen an zwischengeschaltete Server, die als Verstärker (Amplification) dienen. Diese Server werden so ausgewählt, dass ihre Antworten um ein Vielfaches größer sind als die ursprüngliche Anfrage, wodurch die Menge des gesendeten Datenverkehrs erhöht wird. Die missbrauchten Server spiegeln dann die Anfragen und leiten sie in verstärkter Form an das eigentliche Angriffsziel weiter. Reflection-Amplification-Angriffe sind besonders gefährlich, da sie nicht nur die Menge des bösartigen Datenverkehrs erhöhen, sondern auch die Herkunft des Angriffsverkehrs verschleiern.

Im Jahr 2023 hat das LSOC eine Flut von Verstärkertechniken registriert. Viele dieser Angriffstechniken, wie DNS Reflection Amplification und NTP Reflection Amplification, zählen bereits seit 2013 zur Standard-Ausrüstung von DDoS-Angreifern. Diese Techniken zeichnen sich durch eine immense Verstärkung aus, beispielsweise durch eine 100-fache Verstärkung bei DNS-Attacken und eine bis zu 200-fache Verstärkung bei NTP-Angriffen.

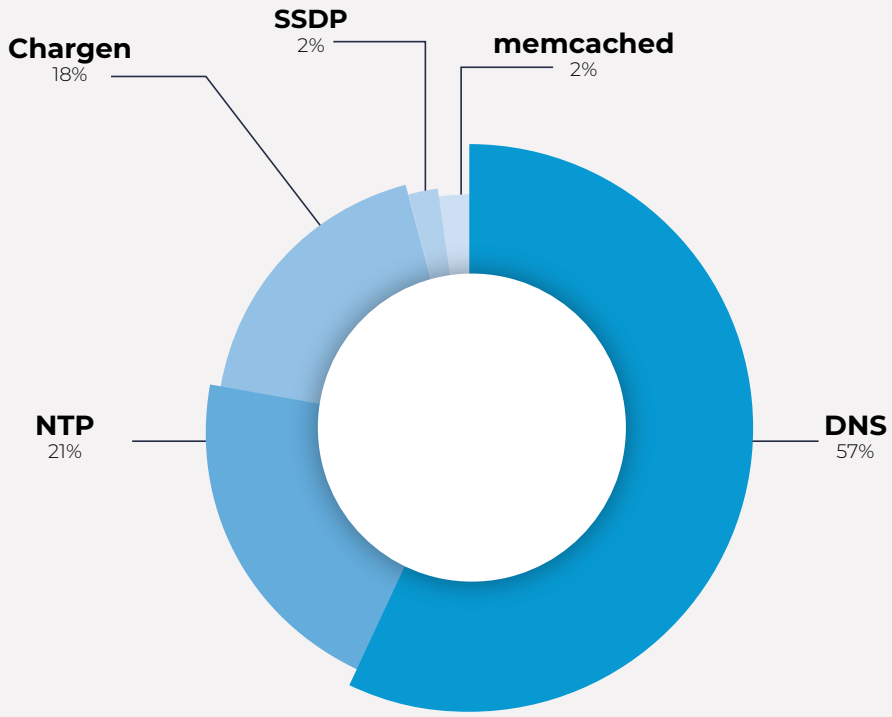
„Noch immer gibt es eine Vielzahl falsch konfigurierter Server und Services im Internet, die Angreifer für Reflection-Amplification-Attacken nutzen. Diese Angriffe sind nicht nur kostengünstig, sondern auch besonders gefährlich, da sie die Herkunft des Angriffes verschleiern und die Zielsysteme überlasten. Es ist daher unerlässlich, dass sich Unternehmen mit sinnvollen und effektiven Maßnahmen gegen solche DDoS-Angriffe schützen.“

Karsten Desler, CTO, Link11 Group

Obwohl Angreifer ständig neue Schwachstellen wie unzureichend geschützte Internetdienste und offene Dienste entdecken, wurden im Betrachtungszeitraum für nahezu alle Angriffe bereits bekannte und altbewährte Vektoren eingesetzt. Der Internetdienst, der 2023 am häufigsten für Angriffe ausgenutzt und als Verstärker missbraucht wurde, war DNS (57 %) gefolgt von NTP (21 %) sowie Chargen (18 %). Nur bei jeweils 2 % der Angriffe wurden Memcached und SSDP als Angriffsvektoren eingesetzt.

DNS und NTP sind zwei fundamentale Systeme des Internets, ohne die keiner der User auskommt. DDoS-Angriffe auf diese beiden Systeme sind kostengünstig und erfolgversprechend. DNS steht für Domain Name System, ein Protokoll, das Domainnamen mit IP-Adressen verknüpft. Bei einer DNS-Amplification-Attacke sendet der Angreifer manipulierte Anfragen an offene DNS-Resolver, die dann große Antworten generieren und das Zielsystem überfordern. Das Missverhältnis zwischen der geringen Anfrage und der großen Antwort wird ausgenutzt, um den Traffic zu verstärken. Das Zielsystem wird mit einem massiven Datenstrom überflutet und der Zugriff auf den Server und seine Infrastruktur blockiert. Durch gefälschte Quell-IP-Adressen bleiben die Angreifer anonym und die Attacken sind vergleichsweise kostengünstig durchzuführen.

Reflection-Amplification-Vektoren 2023



Web Protection

Bot Management: Das Unsichtbare kontrollieren

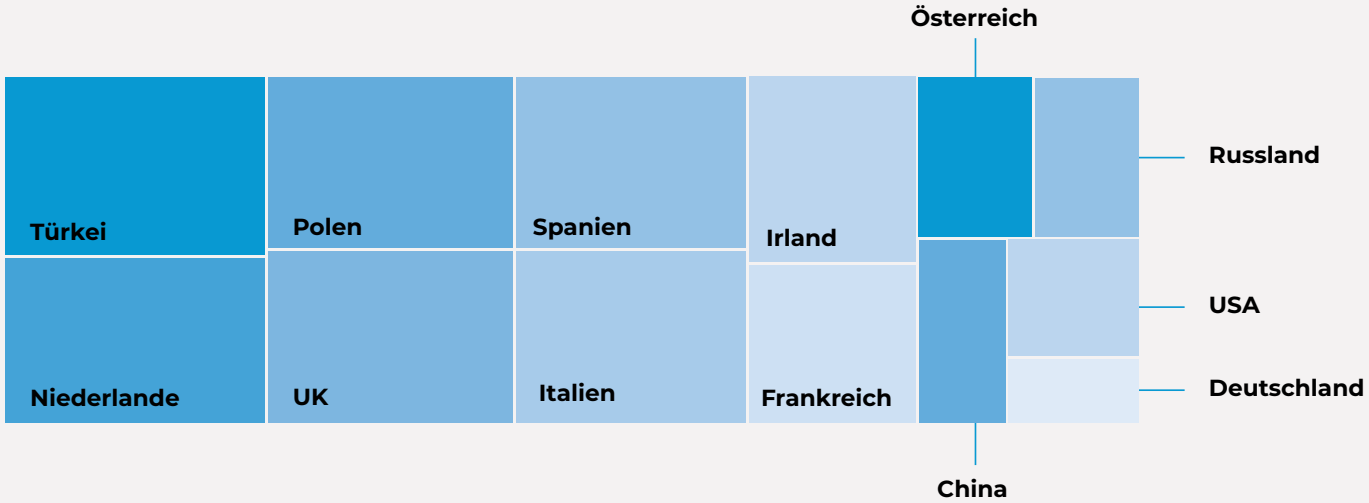
Es gibt gute und böse Bots sowie Botnetze. Was sind die Unterschiede und worauf kommt es, um sich dieser unsichtbaren Armee zu stellen, die sich über das Internet ausbreitet und in vielen Fällen großen Schaden anrichten kann? Es gibt Bots, die zunehmend für automatisierte Prozesse eingesetzt werden, um die Effizienz zu steigern. Dazu gehören etwa SEO-Analyse, Link-Previews, Social-Media-Interaktionen und das Scraping von Daten für Marktanalysen. Diese Bots spielen eine entscheidende Rolle bei der Automatisierung von Aufgaben und der Verbesserung unterschiedlicher betrieblicher Abläufe.

Gleichzeitig werden Bots jedoch auch für betrügerische Aktivitäten genutzt, wie zum Beispiel Spam oder Credential Stuffing. Diese sogenannten „Bad Bots“ sind eine ernsthafte Bedrohung für die Sicherheit von Unternehmen, da sie schädliche Auswirkungen auf Websites und Online-Ressourcen haben können. Umso wichtiger ist es, sich vor diesen Gefahren zu schützen.

Darüber hinaus gibt es auch noch Botnetze. Das sind Netzwerke von kompromittierten Computern oder Geräten, die von Angreifern ferngesteuert werden, ohne dass die Eigentümer davon wissen. Diese Netzwerke können für verschiedene böswillige Zwecke eingesetzt werden, von Spam-Versand bis hin zu groß angelegten DDoS-Angriffen. Diese Netzwerke können enorme Ausmaße annehmen und lange Zeit unentdeckt bleiben. Dadurch können nicht nur Netzwerke überlastet, sondern auch sensible Daten gestohlen und Online-Dienste beeinträchtigt werden.

Laut der Analysten von Forrester[24] kann inzwischen jeder mit einem Internetzugang einen Bot-Angriff starten und dabei werden die Angriffe immer raffinierter. Generative KI hilft den Angreifern, ihre Bot-Armeen immer weiter zu verbessern, sodass der Bedarf an fortschrittlichem und effektivem Schutz für Unternehmen immer größer wird. Dennoch sind laut des aktuellen U.S. Bot Security Reports[25] zwei von drei der untersuchten US-amerikanischen Websites gegen simple Bot-Attacken ungeschützt.

Herkunftsländer der im Link11-Netzwerk registrierten Bad Bots



Unternehmen sehen sich jährlich mit einem beträchtlichen Schaden konfrontiert, der durch Angriffe von Bad Bots auf ihre digitalen Assets entsteht. Laut Juniper Research[26] wird der Online-Betrug durch Bots bis 2027 voraussichtlich um 131 Prozent zunehmen. Die rasante Entwicklung generativer KI-Technologien könnte diesen Anstieg sogar beschleunigen. Von diesem Trend sind Unternehmen aller Branchen betroffen, da automatisierte Angriffe eine zunehmende Bedrohung darstellen.

Dabei gibt es inzwischen eine Vielzahl von Techniken, um menschlichen Datenverkehr vom maschinellen Bot-Traffic zu unterscheiden:

- Verhaltensanalyse: Diese Technik zielt darauf ab, Muster in Benutzeraktivitäten zu identifizieren, da Menschen und Bots sich tendenziell unterschiedlich verhalten. Während ein Mensch zum Beispiel seine Maus bewegt oder scrollt, würde das ein Bot nicht tun.
- CAPTCHA: Benutzer müssen Aufgaben lösen, die für Menschen einfach, aber für Bots schwierig sind. Dazu gehört u.a. das Erkennen von verzerrtem Text oder Bildern.
- IP-Reputation: Eingehender Datenverkehr wird mit bekannten böswilligen IP-Adressen abgeglichen und entsprechend blockiert.
- Künstliche Intelligenz: Mithilfe maschinellen Lernens werden Muster im Datenverkehr analysiert wie etwa Traffic-Logs, um abnormales Verhalten zu erkennen.

Lisa Fröhlich, Unternehmenssprecherin, im Dialog mit Eyal Hayardeny, President, Link11 Group

Was sind die größten Herausforderungen für Unternehmen, wenn wir uns mit Bot Management beschäftigen?

Besonders schwierig ist es, zwischen „guten" und „bösartigen" Bots zu unterscheiden. Nicht jeder automatisierte Datenverkehr ist per se schlecht oder schädlich, gleichzeitig ist eine effektive Lösung nötig, um bösartige Bots zu identifizieren und sie im zweiten Schritt zu entschärfen. Es sollte keinerlei Beeinträchtigungen für den Nutzer geben, obwohl das Volumen des Bot-Verkehrs herkömmliche Sicherheitsmaßnahmen überwältigen kann.

Das ist in der Tat ein heikles Unterfangen. Kannst du einige der häufigsten Arten von Bot-Angriffen erläutern, denen Unternehmen begegnen?

Unternehmen sind mit einer Vielzahl von Bot-Angriffen konfrontiert, die jeweils unterschiedliche Risiken darstellen. DDoS-Angriffe können zu längeren Ausfallzeiten führen, durch Scraping und Credential Stuffing können Daten gestohlen oder Nutzerkonten komplett übernommen werden – die Bedrohungen sind vielfältig und entwickeln sich ständig weiter. Außerdem kann es im E-Commerce-Bereich zum Horten von Warenbeständen oder Klickbetrug in der digitalen Werbung kommen.

Es gibt viele verschiedene Bot-Angriffe. Gibt es denn Branchen, die besonders betroffen sind?

Auf jeden Fall. Die Bedrohungsszenarien variieren von Branche zu Branche. Sie spiegeln auch die unterschiedlichen Motivationen der Cyberkriminellen wider. E-Commerce-Websites haben ein größeres Risiko für das Horten von Beständen, Finanzinstitute hingegen kämpfen gegen den Missbrauch von Formularen. Unternehmen im Gesundheitswesen sind eher mit dem Auslesen von Patientendaten konfrontiert, während Unternehmen digitaler Medien sich gegen Klickbetrug wehren müssen.

Was sind die Hauptmotive für Bot-Angriffe?

Die Motive für Bot-Angriffe sind vielfältig, sie reichen von finanzieller Motivation bis hin zu Wettbewerbsvorteilen. Bedrohungsakteure versuchen, gestohlene Daten zu verkaufen, Konkurrenten zu unterbieten oder Geschäftsabläufe zu stören. Staatlich unterstütze Angreifer können zudem auch Spionage und Sabotage betreiben. Diese verschiedenen Motive sind der Schlüssel, die potenziellen Gefahren zu antizipieren und die Bot-Angriffe wirksam zu entschärfen.

Welche Strategien sollten Unternehmen anwenden, um die von Bot-Angriffen ausgehenden Risiken zu minimieren?

Das einzigartige Risikoprofil der einzelnen Branchen ist entscheidend, um die passende Verteidigungsstrategie einzusetzen. Hier ist ein vielschichtiger Ansatz erforderlich. Neben fortschrittlichen Technologien zur Erkennung der bösartigen Bots ist die Implementierung robuster Authentifizierungsmaßnahmen wie die Multi-Faktor-Authentifizierung notwendig, um die Risiken zu reduzieren. Unternehmen sollten auch ihre Sicherheitsprotokolle regelmäßig aktualisieren, um neuen Bedrohungen wirksam zu begegnen und mit Sicherheitsexperten zusammenarbeiten. Darüber hinaus sollte das Sicherheitsbewusstsein bei den Mitarbeitenden kontinuierlich gefördert werden.

Sneaker Bots: Wenn Schuhe zu Beute werden

In der Welt der „Limited Editions“ von Sneakern kommt es oft zu einem Wettlauf gegen die Zeit. Tausende Nutzer warten ungeduldig auf einer Landingpage oder in einem virtuellen Warteraum, um eines der begehrten Einzelstücke zu ergattern. Für viele endet dieses Unterfangen ziemlich enttäuschend – ohne den Wunschturnschuh, denn andere Nutzer betreiben ein lukratives Geschäft: Sie kaufen die meisten dieser Schuhe auf, um sie auf alternativen Märkten weiterzuverkaufen. Dabei setzen sie auf „Sneaker Bots“, die den Kauf mehrerer Artikel automatisieren.

Das Geschäftsmodell hinter diesen Bots ist ebenso einfach wie profitabel: Die Betreiber verfügen über Lizenzen, die in begrenzter Anzahl angeboten werden und erzielen damit Gewinne in Höhe von mehreren tausend Dollar pro Lizenz. Die Bot-Betreiber wiederum verlassen sich darauf, dass sie die erworbenen Schuhe in alternativen Märkten weiterverkaufen können, um ihren Gewinn zu realisieren.

Um ihre Identität zu verschleiern und Sicherheitsmechanismen zu umgehen, bedienen sich die Betreiber dieser Bots ausgeklügelter Techniken. Durch den Einsatz von privaten Proxys bleiben ihre IP-Adressen blockiert, während andere Online-Dienste sogar Telefonnummern für SMS und alternative Lieferoptionen anbieten, um die Verwendung einer einzigen Lieferadresse zu vermeiden.

Indem sie solche ausgefeilten Mechanismen und APIs nutzen, missbrauchen die Sneaker Bots das Backend von E-Shops, um menschliche Nutzer zu imitieren, Sicherheitsmechanismen zu umgehen und letztlich diese Art von Betrug zu ermöglichen.

Die rechtliche Situation ist in den meisten Ländern diffus: Die Verwendung einer alternativen API zum direkten Kauf von Artikeln statt über die eigentliche Schnittstelle ist eine rechtliche Grauzone. Solange die gekauften Artikel bezahlt werden, ist es schwierig das rechtlich zu verfolgen.

Was verbirgt sich hinter automatisiertem Datenverkehr?

Automatisierter Datenverkehr auf einer Website bedeutet einen Verbrauch von Rechenressourcen. Je nachdem, wer die Daten anfordert, kann das sowohl positiv als auch negativ sein: Bots und Software von Partnern und bekannten Organisationen können einen Nutzen bringen, während unbekannte Bots eine Grauzone darstellen. Im Link11-Netzwerk sind rund 65 % des beobachteten Traffics maschinellen Ursprungs.

Einige legitime Modelle nutzen automatisierten Verkehr: Indizes und Dienste, die Crawler einsetzen, oder Dienste, die Testverkehr anbieten. Auf der anderen Seite existieren auch illegitime Modelle, die auf automatisiertem Verkehr im Internet basieren. Dazu gehören Betrugsmethoden wie Credential Stuffing, das dazu dient, Datensätze gestohlener Konten zu validieren, oder Techniken zur Kontoübernahme. Darüber hinaus gibt es illegale Märkte und Sniping-Bots, die beispielsweise limitierte Schuhe oder Kryptowährungen zu niedrigen Preisen erwerben.

Das Problem von Credential Stuffing und Betrug ist weit verbreitet und einfach durchzuführen. Innerhalb weniger Minuten können im Dark Web Daten und Dienste gefunden werden, die Betrug ermöglichen. Um dem entgegenzuwirken, ist es entscheidend, zwischen guten und schlechten Bots auf unseren Websites zu unterscheiden. Eingebaute Resilienzschichten zur Validierung von Kunden bieten nicht nur einen Mehrwert für die Datenspeicherung, sondern verbessern auch unsere Sicherheitslage. Die Prävention von Kundenkonteneinbrüchen oder unerwünschten Übernahmen verringert zudem die Wahrscheinlichkeit von Rechtsstreitigkeiten.

Account Takeover: Die Gefahr gestohlener Zugangsdaten

Die Weiterentwicklung von Bot-Technologien ist alarmierend. Früher waren Bots einfache Tools für Phishing-E-Mails, doch heute sind sie hochentwickelt und können menschliches Verhalten nachahmen, was ihre Erkennung erschwert. Zwischen 2021 und 2022 hat sich der Anteil hochentwickelter Bad Bots verdoppelt und dominiert nun den weltweiten Datenverkehr.

Die folgende Grafik zeigt auf, welchen Ursprung die im Link11-Netzwerk registrierten Bad Bots haben. Die meisten aller Bots finden ihren Weg über Datenzentren, zu je gleichen Teilen kommen die Bots über klassische und mobile Telekommunikationswege. Außerdem spielen noch Software und Hosting-Provider eine Rolle. Im Grunde waren dies die erwarteten Ergebnisse, doch warum kommen so viele Bad Bots über den mobilen Datenverkehr?

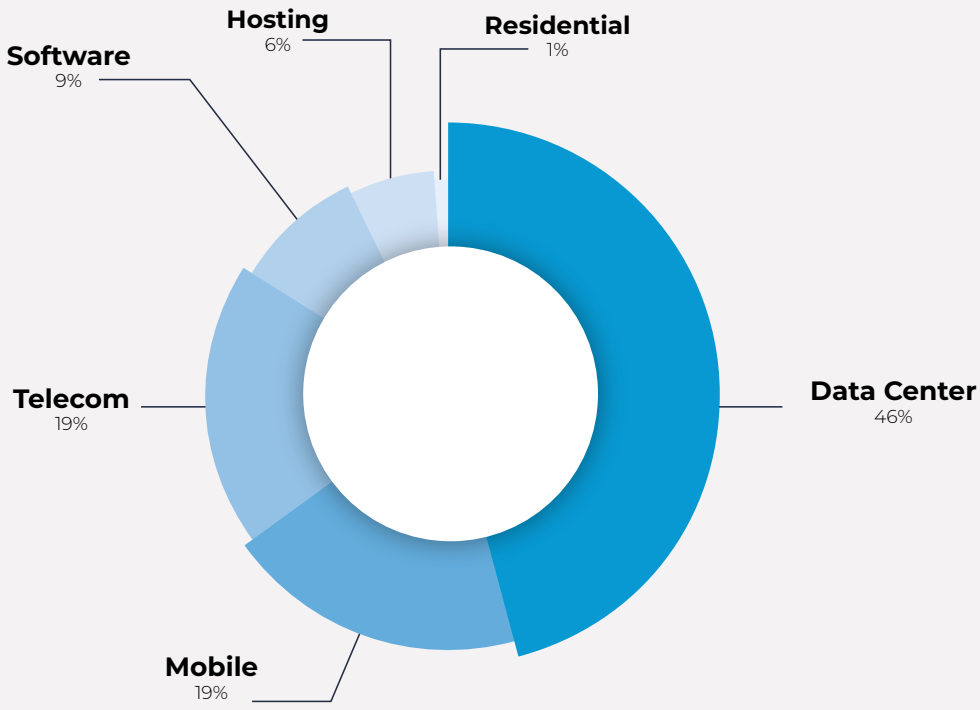
Dafür gibt es zwei Erklärungen:

1. Mobilanwendungen gehören inzwischen zu einem der Hauptangriffsziele für Bad Bots: Jede Mobilanwendung bringt ihre eigene Programmierschnittstelle mit sich, kurz API. Diese sind besonders gefährdet. Cyberkriminelle können diese APIs mit verschiedenen Möglichkeiten angreifen. Dazu gehört u. a. das API-Reverse-Engineering oder spezielle Automatisierungssoftware. Umso wichtiger ist der Schutz der Smartphone-App-APIs.

2. Die Anzahl von böswilligen Bots, die von Mobiltelefonen ausgehen, hat in jüngster Zeit zugenommen.[27] Die als Badbox und Peachpit bekannte Android-Malware hat Tausende von Geräten infiziert. Diese Malware wird bereits vor dem Versand auf den Geräten installiert und verbreitet sich über preiswerte Set-Top-Boxen und ähnliche Android-Geräte. Sie zielt darauf ab, Betrugsschemata umzusetzen und Geräte durch Werbebetrug sowie die Installation von schädlichem Code zu infizieren.

Cyberkriminelle werden sich in Zukunft stärker darauf konzentrieren, API-Endpunkte und mobile Anwendungen mit ausgefeilter Automatisierung anzugreifen. Zu einem solchen Angriff gehören die sogenannten Account Takeovers (ATO). Bei ATO-Angriffen versuchen Hacker, sich Zugang zu legitimen Online-Konten zu verschaffen. Die Zahl von Account-Takeovers ist zwischen 2021 und 2022 bereits um 155 % gestiegen.[28] Erfolgreiche ATOs können potenziell verheerende Folgen haben. Über diesen Weg werden Identitäten gestohlen, mit denen die Angreifer in die anvisierten Systeme eindringen können. Dadurch können Daten gestohlen werden, Betrug stattfinden oder andere kriminelle Aktivitäten durchgeführt werden.

Ursprung der im Link11-Netzwerk registrierten Bad Bots



Der Zugang zu betrügerischen Daten und Diensten ist erschreckend einfach: Eine fünfminütige Suche im Dark Web genügt, um Dumps zu finden oder Dienste zu erwerben, die sogar mit Preislisten aufwarten. Dies führt dazu, dass einige Konten direkt missbraucht werden können, um Betrug zu begehen oder gezielte Angriffe auf Organisationen vorzubereiten. Die Kontoübernahme wird dabei nicht unbedingt von einem Bot durchgeführt, sondern oft von Menschen, die die gesammelten Informationen nutzen, um ausgewählte Konten zu übernehmen und betrügerische Aktivitäten durchzuführen.

Unter „Dumps“ versteht man im Zusammenhang mit betrügerischen Aktivitäten Daten, die aus gestohlenen Kredit- oder Debitkarten extrahiert wurden. Diese Daten enthalten in der Regel Informationen wie Karteninhabername, Kartennummer, Ablaufdatum und möglicherweise sogar die Sicherheitscodes. Betrüger können diese Informationen nutzen, um betrügerische Transaktionen durchzuführen oder Konten zu übernehmen. Das Finden und der Handel mit Dumps sind daher eine gängige Praxis im Bereich des Cyberbetrugs.

Um die Organisation zu schützen, ist eine Strategie zur Wahrung der Vertraulichkeit, Integrität und Authentizität von Informationen unerlässlich. Die folgenden Abwehrmaßnahmen sind die drei wichtigsten, wenn es gilt Account Takeover-Angriffe zu verhindern:

Multi-Faktor-Authentifizierung: Stärkung der Sicherheit von Benutzerkonten

Die Multi-Faktor-Authentifizierung (MFA) ist ein entscheidendes Instrument, um die Sicherheit von Benutzerkonten zu erhöhen. Das Anfordern mehrerer Nachweise für die Benutzeridentität reduziert die Wirksamkeit von gestohlenen Zugangsdaten erheblich. Die Kombination verschiedener Authentifizierungsfaktoren bietet eine robuste Verteidigungslinie gegen ATO-Angriffe. Durch die Nutzung verschiedener MFA-Mechanismen können Organisationen die Sicherheit ihrer Systeme weiter erhöhen.

Phishing-Prävention: Mehrschichtige Verteidigung

Phishing ist eine weit verbreitete und gefährliche Form von Social Engineering, die darauf abzielt, dass Menschen sensible Informationen preisgeben. Eine wirksame Phishing-Prävention umfasst mehrere Verteidigungsmaßnahmen. Dazu gehören etwa das Erhöhen des Sicherheitsbewusstseins und das Filtern von Phishing-Nachrichten. Durch die Implementierung einer robusten Anti-Phishing-Strategie können Organisationen das Risiko von ATO-Angriffen erheblich verringern.

Rate Limiting: Technologie zur Verhinderung von ATO

Rate Limiting ist ein wichtiger Bestandteil der ATO-Abwehrstrategie. Eine robuste Web-Application and API Protection-Lösung (WAAP) überwacht die Rate, mit der Clients Anfragen an die geschützte Backend-Umgebung senden. Wenn eine bestimmte Datenquelle innerhalb eines definierten Zeitraums zu viele Anfragen sendet, kann diese Datenquelle für einen festgelegten Zeitraum von weiterem Zugriff ausgeschlossen werden. Die Überwachung und Begrenzung der Anfragerate schränken den Zugriff von potenziellen Angreifern ein. Somit wird die Wirksamkeit von ATO-Angriffen reduziert.

„Es ist erschreckend einfach. Mit nur wenigen Minuten Recherche im Dark Web können Betrüger problemlos Daten wie gestohlene Kontodaten finden oder Dienste in Anspruch nehmen, die ihnen bei ihren kriminellen Aktivitäten helfen. Deshalb ist es wichtig, die Anfragen von Bots und anderen automatisierten Systemen zu überwachen, um potenzielle Angriffe frühzeitig zu erkennen und zu verhindern. Eine umfassende Strategie zur Wahrung der Vertraulichkeit, Integrität und Authentizität von Informationen ist unerlässlich, um das Risiko von Account Takeover-Angriffen zu minimieren.“

Mattia Rambelli, Solutions Engineer, Link11

Die Überprüfung der Kundenanfragen auf einer Website und das Verständnis dafür, ob die Anfragen von Botnetzen kommen, können helfen, Vorfälle zu verhindern. Darüber hinaus ist es wichtig, die Anfragen von Bots und anderen automatisierten Systemen zu überwachen, um potenzielle Angriffe frühzeitig zu erkennen und zu verhindern. Letztlich ist jedoch eine differenzierte Herangehensweise an die Herausforderungen des automatisierten Datenverkehrs entscheidend, um sowohl die Sicherheit als auch die Effizienz von digitalen Plattformen zu gewährleisten.

Bei der Auswahl des Bot Managements sind daher einige Merkmale zu beachten:

KI und maschinelles Lernen: Moderne Tools sollten KI und maschinelles Lernen nutzen, um sich kontinuierlich weiterzuentwickeln und weiterhin neue Bedrohungen zu erkennen.

Integration mit bestehenden Systemen: Ein gutes Werkzeug integriert sich nahtlos in Ihre IT-Infrastruktur und Sicherheitstools, um Sicherheitslücken zu vermeiden.

Einfache Bereitstellung und Wartung: Die Installation sollte einfach sein und das Werkzeug sollte einen umfassenden Schutz bieten, ohne ständige Wartung zu erfordern.

Flexibilität und Anpassungsfähigkeit: Es sollte möglich sein, das Werkzeug an Ihre spezifischen Anforderungen anzupassen und benutzerdefinierte Regeln zu erstellen.

Datenschutzkompatibilität: Stellen Sie sicher, dass das Werkzeug mit geltenden Datenschutzframeworks kompatibel und flexibel genug ist, um zukünftige Compliance-Änderungen zu bewältigen.

Echtzeitüberwachung: Das Werkzeug sollte jede Anfrage in Echtzeit überwachen können, um potenzielle Bedrohungen sofort zu erkennen und darauf zu reagieren.

Skalierbarkeit: Es sollte in der Lage sein, auch bei einem Anstieg des Datenverkehrs ohne Beeinträchtigung der Kundenerfahrung zu skalieren.

„Bot Management ist eine komplexe Herausforderung für Unternehmen in einer zunehmend digitalisierten Welt. Durch einer Kombination aus technischen Sicherheitsvorkehrungen, Überwachung des Datenverkehrs und Aufklärung der Mitarbeiter können Unternehmen ihre Systeme vor den Auswirkungen schädlicher Bots schützen und gleichzeitig die Vorteile automatisierter Prozesse nutzen.“

Ziv Grinberg, VP Product Management, Link11 Group

WAF: Zuverlässiger Schutzschild für Sicherheit im Web

Im Jahr 2023 kam es erneut zu einem alarmierenden Anstieg an gemeldeten Sicherheitslücken. Laut des Netzwerkausrüsters Cisco verzeichnete die CVE-Datenbank 2023 einen Zuwachs von fast 29.000 Einträgen, was einem Anstieg von 15 % gegenüber dem Vorjahr entspricht.[29] Jede kritische Sicherheitslücke in Form von nicht gepatchter Software ist ein potenzielles Einfallstor für Cyberkriminelle.

Besonders Web-Applikationen stellen ein großes Sicherheitsrisiko dar. Cyberkriminelle nutzen immer ausgefeiltere Methoden, um Schwachstellen in solchen Anwendungen auszunutzen und auf vertrauliche Daten zuzugreifen oder diese zu manipulieren.

Die Verwendung einer herkömmlichen Firewall reicht oft nicht aus, um Webanwendungen effektiv zu schützen. Diese kann zwar den Datenverkehr überwachen und unautorisierte Zugriffe blockieren, ist jedoch nicht in der Lage, Angriffe auf die Anwendungslogik selbst zu erkennen und abzuwehren. Hier kommt die Web-Application Firewall (WAF) ins Spiel. Im Link11-Netzwerk werden täglich rund 180.000 abgeschwächte WAF-Ereignisse registriert.

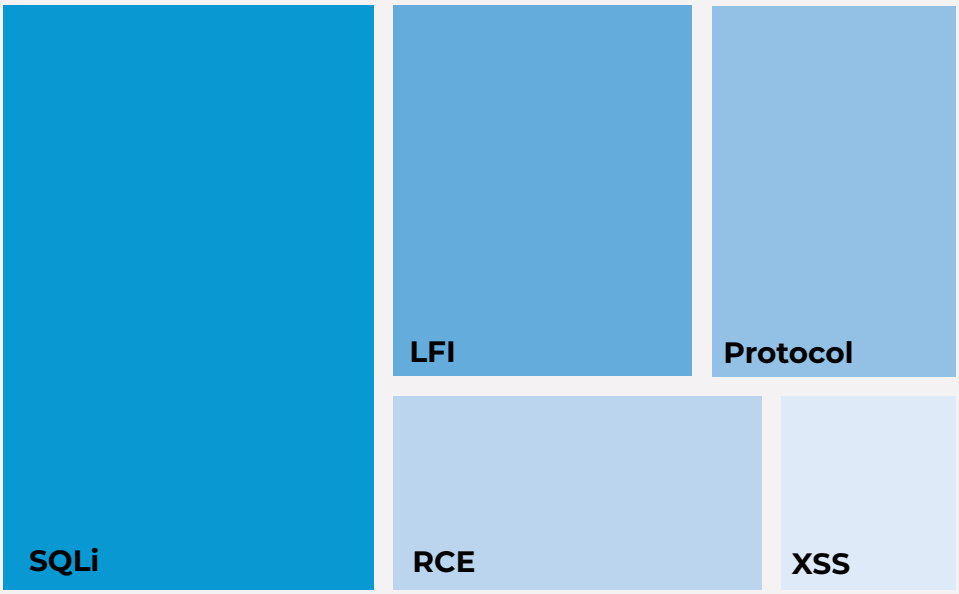
Eine WAF ist darauf ausgelegt, den Datenverkehr auf Anwendungsebene zu überprüfen und verdächtige Aktivitäten zu erkennen, bevor sie die Webanwendung erreichen. Sie kann beispielsweise ungewöhnliche Benutzereingaben identifizieren, die auf mögliche Angriffe wie SQL-Injection oder Cross-Site Scripting hindeuten könnten. Durch die Analyse des Datenverkehrs auf der Ebene der HTTP-Pakete kann eine WAF potenziell schädliche Anfragen blockieren oder den Benutzer alarmieren.

Der Einsatz einer WAF ist besonders wichtig in Bereichen wie dem Zahlungsverkehr, wo Unternehmen verpflichtet sind, strenge Sicherheitsstandards einzuhalten. Kreditkartenfirmen und andere Zahlungsdienstleister fordern zum Beispiel von Webshop-Betreibern den Einsatz einer WAF, um die Vertraulichkeit und Integrität der Zahlungsdaten ihrer Kunden zu gewährleisten.

Zudem bietet die aktive Überwachung und regelmäßige Überprüfung von Webanwendungen einen wichtigen Schutzmechanismus gegen potenzielle Bedrohungen. Durch die Identifizierung und Behebung von Sicherheitslücken können Unternehmen das Risiko von Datenverlusten, Betriebsunterbrechungen und Reputationsschäden minimieren.

Zu den Top 5 im Link11-Netzwerk registrierten Angriffen auf Web-Applikationen gehören die folgenden Angriffe:

Top-5 Angriffe auf Web-Applikationen



SQL-Injection (SQLi) ist eine Sicherheitslücke, bei der Angreifer schädlichen SQL-Code in Webanwendungen einschleusen, um die zugrunde liegende Datenbank zu manipulieren. Das gelingt etwa, wenn Benutzereingaben nicht ausreichend validiert werden. Indem Angreifer manipulierte SQL-Befehle in Eingabefelder oder URL-Parameter einschleusen, können sie die Ausführung von unerwünschten SQL-Abfragen auslösen. So können die Angreifer, Datenbankabfragen modifizieren, auf vertrauliche Informationen zugreifen oder die gesamte Datenbank kompromittieren. Durch das Einschleusen von zusätzlichen SQL-Befehlen können außerdem Daten extrahiert, geändert oder gelöscht werden, was erhebliche Sicherheitsrisiken für die betroffene Anwendung und ihre Benutzer darstellt.

Die Local File Inclusion-Attacke (LFI) ist eine Web-Schwachstelle, durch die ein Angreifer auf Dateien auf dem Server zugreifen kann, die normalerweise nicht für die Öffentlichkeit bestimmt sind. Das können zum Beispiel Passwortdateien oder Quellcode sein. Ein Angreifer kann diese Lücke nutzen, indem er die URL der Webseite manipuliert, um Zugriff auf solche Dateien zu erhalten. Dadurch kann der Angreifer sich sensible Informationen anzeigen lassen oder sie herunterladen. Das kann schwerwiegende Sicherheitsprobleme wie Cross-Site-Scripting (XSS) und Remote-Code-Ausführung zur Folge haben. Um solche Angriffe zu verhindern, müssen Entwickler sicherstellen, dass die Website korrekt programmiert ist und dass keine Benutzereingaben direkt auf Dateipfade angewendet werden können.

Cross-Site-Scripting (XSS) ist ein Angriffstyp, bei dem Angreifer bösartigen Code in eine scheinbar vertrauenswürdige Webseite einschleusen. Das gelingt sowohl über Webformulare als auch URLs und kann verschiedene Schäden verursachen. Dazu gehört die Beeinträchtigung der angegriffenen Website bis hin zum Diebstahl von Benutzerdaten wie Passwörtern. Es gibt drei Arten von XSS-Angriffen: reflektierte, persistente und DOM-basierte Angriffe. Bei reflektiertem XSS sendet der Angreifer den Code an den Server, der ihn dann an das Opfer zurückgibt. Bei persistentem XSS wird der Code auf dem Server gespeichert und allen Besuchern der Seite angezeigt. Bei DOM-basiertem XSS wird der Code direkt im Browser des Opfers ausgeführt.

Remote Code Execution (RCE) bezeichnet die Möglichkeit, bösartigen Programmcode auf einem Computer oder Gerät über ein Netzwerk wie das Internet aus der Ferne auszuführen. Diese Art von Angriffen resultiert oft aus Sicherheitslücken in Betriebssystemen, Anwendungen oder unsicher gestalteten Eingabemasken. Cyberkriminelle nutzen RCE, um sich unberechtigten Zugriff auf Systeme zu verschaffen, Malware einzuschleusen, sensible Daten zu stehlen oder sogar vollständige Kontrolle über die betroffenen Systeme zu erlangen. Dabei ist kein physischer Zugriff auf die Geräte nötig, da die Angriffe über das Internet erfolgen.

Protokollangriffe umfassen verschiedene Techniken, die darauf abzielen, Schwachstellen in Kommunikationsprotokollen auszunutzen, um Webanwendungen oder Server zu kompromittieren. Dazu gehören:

- **HTTP-Response-Splitting:** Bei diesem Angriff werden HTTP-Antworten so manipuliert, dass sie in mehrere Teile zerlegt werden. Auf diese Weise können Angreifer zusätzliche Inhalte oder Header einschleusen, die vom Server oder zwischengeschalteten Instanzen möglicherweise anders interpretiert werden.
- **HTTP-Smuggling:** HTTP-Smuggling-Angriffe nutzen Unterschiede in der Art und Weise aus, wie Frontend- und Backend-Server HTTP-Anfragen behandeln und interpretieren. Dadurch können Angreifer Sicherheitsmechanismen umgehen und potenziell bösartige Aktionen ausführen.
- **HTTP-Header-Injection:** Angreifer fügen nicht autorisierte HTTP-Header in Anfragen oder Antworten ein, um das Serververhalten zu manipulieren oder Schwachstellen in Webanwendungen auszunutzen. Dies kann zu verschiedenen Sicherheitsproblemen wie Cross-Site Scripting (XSS) oder Remote Code Execution (RCE) führen.
- **HTTP-Parameter-Pollution (HPP):** Bei HPP-Angriffen manipulieren Angreifer Parameter in HTTP-Anfragen, um die serverseitige Verarbeitungslogik zu verwirren oder zu umgehen. Dies kann zu unerwartetem Verhalten wie Privilegien-Eskalation, Informationslecks oder Denial-of-Service-Angriffen führen.

„Web-Application Firewalls sind entscheidend im Kampf gegen Webanwendungsangriffe. Sie bieten proaktiven Schutz und minimieren Risiken, indem sie Anomalien erkennen und verdächtige Aktivitäten blockieren. Damit kann die Sicherheit und Integrität von Webanwendungen langfristig gewährleistet werden."

Ziv Grinberg, VP Product Management, Link11 Group

Neben dem Blockieren schädlicher Anfragen können Web-Application Firewalls (WAF) jedoch vieles mehr:

1. **Schutz vor Zero-Day-Angriffen:** WAFs nutzen Signaturen und Verhaltensanalysen, um Web-Traffic-Anomalien zu erkennen und verdächtige Aktivitäten zu blockieren, auch ohne spezifische Signaturmuster für bekannte Angriffe. Dadurch werden Zero-Day-Angriffe abgewehrt, die neue Schwachstellen ausnutzen, für die noch keine Patches verfügbar sind.
2. **Filterung von Benutzereingaben:** WAFs können Benutzereingaben überprüfen und validieren, um potenziell schädlichen Code zu identifizieren und zu blockieren. Dies kann helfen, Injection-Angriffe per SQL und Command zu verhindern, indem schädliche Befehle oder Skriptfragmente blockiert werden.
3. **Schutz vor Skriptangriffen:** Einige WAFs bieten Funktionen zur Erkennung und Blockierung von bösartigen Skripten, die in Webseiten eingebettet sind, wie beispielsweise Cross-Site-Scripting (XSS). Durch das Filtern von Skriptinhalten können WAFs dazu beitragen, die Ausführung von schädlichem Code im Browser von Benutzern zu verhindern.
4. **Content- und Dateifilterung:** WAFs können den Inhalt eingehender Dateien überprüfen, einschließlich hochgeladener Dateien, um potenziell schädliche Dateien zu erkennen und zu blockieren. So können Angriffe verhindert werden, bei denen Angreifer bösartige Dateien hochladen und ausführen, um etwa eine Remote Code Execution zu erreichen.
5. **Schutz vor Bot-Angriffen:** WAFs können auch dazu beitragen, Bot-Angriffe abzuwehren. Sie erkennen Anomalien im Web-Traffic wie automatisierte Anmeldeversuche und können Denial-of-Service-Angriffe identifizieren sowie blockieren.

Indem sie den Datenverkehr auf Anwendungsebene analysiert, ermöglicht eine WAF eine granulare Kontrolle über den Zugriff auf die Webanwendung. Dies bedeutet, dass Unternehmen individuelle Sicherheitsrichtlinien festlegen können, um bestimmte Arten von Anfragen oder Benutzerverhalten zu blockieren oder je nach den spezifischen Anforderungen ihrer Anwendung und ihres Geschäfts zuzulassen.

Damit eine WAF die unternehmenseigenen Sicherheitsmaßnahmen sinnvoll ergänzen und so effektiv wie möglich schützen kann, sind einige wichtige Punkte zu berücksichtigen:

1. **Konfiguration und Aktualisierung:** Um neue Bedrohungen und Angriffsmuster zu erkennen, muss die WAF ordnungsgemäß konfiguriert sein und regelmäßig aktualisiert werden.
2. **Whitelisting und Blacklisting:** Basierend auf IP-Adressen, URL-Pfaden, User-Agenten und anderen Parametern können unerwünschter Traffic gefiltert und potenziell schädliche Anfragen blockiert werden.
3. **Input Validation:** Benutzereingaben sollten überprüft und validiert werden. Dadurch können potenziell schädliche Eingaben frühzeitig erkannt und blockiert werden.
4. **Web-Application Security Policies:** Über die Definition klarer Sicherheitsrichtlinien können die Anwendungen an spezifische Bedrohungsmodelle angepasst werden.
5. **Logging und Monitoring:** Verdächte Aktivitäten zu protokollieren hilft dabei, Anomalien oder ungewöhnliche Muster zu erkennen. Durch das regelmäßige Monitoring können potenzielle Angriffe frühzeitig erkannt werden.
6. **Regelmäßige Überprüfungen und Audits:** Mit regelmäßigen Audits der WAF-Konfiguration kann sichergestellt werden, dass sie aktuellen Best Practices und Sicherheitsstandards entspricht.

Web Performance

CDN: Beschleunigung und Sicherheit für jede Online-Präsenz

Website-User erwarten Geschwindigkeit und Sicherheit. Gerade in diesem Zusammenhang kann ein Content Delivery Network (CDN) eine entscheidende Rolle für Unternehmen spielen. Ein CDN trägt dazu bei, die Ladezeiten von Websites zu verkürzen, die Serverlast zu reduzieren und gleichzeitig die Sicherheit zu erhöhen. Ein CDN funktioniert, indem es Inhalte wie Bilder, Videos und Skripte auf Servern in verschiedenen geografischen Regionen speichert und sie dann basierend auf dem Standort des Benutzers wieder ausliefert.

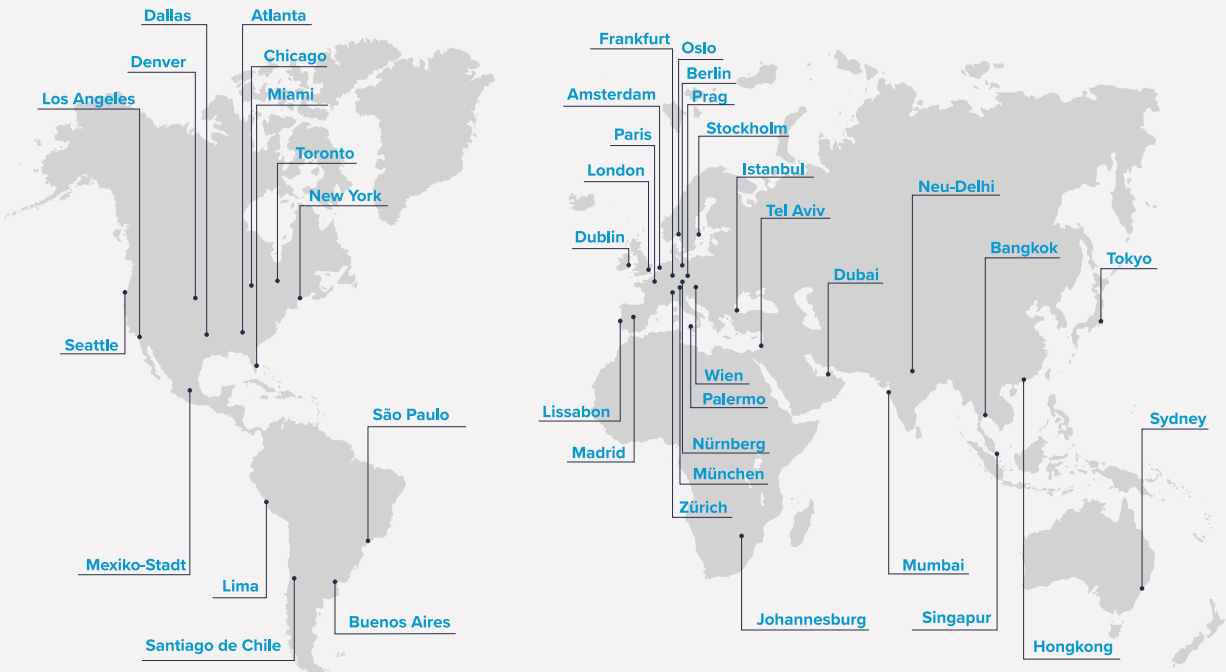
Für die Online-Präsenz der Unternehmen heißt das, dass ein CDN die Latenzzeiten durch kürzere Ladezeiten reduzieren und eine bessere Benutzererfahrung ermöglichen kann. Zudem können die Datenübertragungskosten durch einen optimierten Übertragungsweg verringert werden. Darüber hinaus kann ein CDN die Serverlast des Ursprungs verringern, da mehr Inhalte von den CDN-Servern ausgeliefert werden. Das bedeutet weitere eingesparte Kosten bei der eigenen Hardware.

Link11 bietet jedoch nicht nur eine verbesserte Leistung durch den CDN, sondern integriert auch Sicherheitsfunktionen, die Unternehmen vor Bedrohungen wie DDoS-Angriffen schützen. Durch den Einsatz von Layer 3- und Layer 4-Filterclustern werden CDN-Knoten vor solchen Angriffen geschützt. Die sogenannte Site Shield-Funktion schützt hingegen den Ursprung des Kunden vor direkten Angriffen. Diese nahtlose Integration von CDN und Sicherheitsschicht gewährleistet eine kontinuierliche Verfügbarkeit der CDN-Knoten und bietet einen zusätzlichen Schutz für die Infrastruktur.

Compliance- bzw. Datenschutzvorschriften können ein entscheidender Aspekt sein, um ein CDN zu nutzen. Als europäisches Unternehmen erfüllt Link11 bereits die strengen Anforderungen der DSGVO. Darüber hinaus ermöglicht die Geo-Blocking-Funktion eine präzise Kontrolle darüber, welche Benutzer aus welchen geografischen Regionen auf bestimmte Inhalte zugreifen können, was die Einhaltung spezifischer Datenschutzvorschriften erleichtert. Durch die Kombination von Geo-Fencing und Geo-Blocking können Kunden genau festlegen, welche CDN-Knoten für die Bereitstellung von Inhalten verwendet werden sollen, und so sicherstellen, dass Inhalte nur in ausgewählten Regionen verteilt werden.

Aktuell bietet Link11 drei verschiedene Optionen für die Verarbeitung des Traffics über das CDN in Kombination mit dem WAAP Security Proxy. Diese reichen von einer vollständigen Seitenzwischenspeicherung und WAAP-Schutz für maximale Sicherheit bis hin zu einer statischen Zwischenspeicherung und teilweisem WAAP-Schutz für eine ausgewogene Kombination aus Leistung und Sicherheit. Die Wahl der Konfiguration hängt von den individuellen Anforderungen und Prioritäten des Unternehmens ab.

Weltweites Link11-Netzwerk



Lisa Fröhlich, Unternehmenssprecherin, im Dialog mit Lukas Frank, Product Manager, Link11 Group

Viele Unternehmen unterliegen strengen Compliance-Vorschriften oder Datenschutzgesetzen. Aus diesem Grund wollen viele Nutzer sensible Daten nicht außerhalb der EU auf Servern speichern. Deshalb könnten Kunden daran interessiert sein, die CDN-Knoten entsprechend auszuwählen. Gehen mit der eigenen Auswahl der CDN-Knoten Sicherheits- oder Geschwindigkeitseinbußen einher? Wenn ja, welche?

Die eigene Auswahl der CDN-Knoten kann sich sowohl auf die Geschwindigkeit als auch auf die Leistung der Webseite auswirken. Wenn es weniger Nodes gibt, auf die aus bestimmten Regionen zugegriffen wird, kann das Performanceeinbußen zur Folge haben. Benutzer aus weiter entfernten Regionen müssen auf Knoten in anderen Regionen zugreifen, was zu längeren Ladezeiten führt. Generell sollte jedoch auch in diesem Szenario die Performance mit CDN besser sein als ohne. Die Auswahl der Knoten hat in erster Linie Auswirkungen auf die Performance und weniger auf die Sicherheit.

Sinkt bei der Nutzung eines CDN bei einem DDoS-Angriff automatisch auch die Wahrscheinlichkeit eines Webseitenausfalls, weil Überlastungen vermieden werden?

Das ist richtig. Wird ein CDN genutzt, sinkt während eines DDoS-Angriffs automatisch die Wahrscheinlichkeit eines Webseitenausfalls. Das CDN kann Überlastungen abfedern. Einige DDoS-Angriffe können auf den CDN-Nodes teilweise abgemildert werden, insbesondere durch den Einsatz von Layer 3/4-Schutzmaßnahmen. Darüber hinaus sind die Webseiteninhalte bereits zwischengespeichert. Das bedeutet, dass die User weiterhin auf diese zwischengespeicherten Inhalte zugreifen können, selbst wenn der Origin-Server aufgrund des Angriffs nicht reagiert.

Wie funktioniert der Lastausgleich in einem CDN?

Der Lastausgleich in einem CDN funktioniert unabhängig von Load Balancing, obwohl beide Konzepte miteinander verknüpft werden können. Der Lastausgleich im CDN zielt darauf ab, den Verkehr von der Origin-Server-Infrastruktur zu verringern. Durch die Verteilung von Anfragen auf die verschiedenen CDN-Knoten und das Zwischenspeichern von Inhalten auf diesen Knoten wird die Belastung des Ursprungsservers erheblich reduziert.

Gibt es Probleme bei der Einhaltung der DSGVO durch die Übertragung der IP an einen Replica Server? Wo wird dieser gehostet?

Die Übertragung von IP-Adressen an einen Replica-Server in einem CDN kann theoretisch Probleme in Bezug auf die Einhaltung der DSGVO aufwerfen, da IP-Adressen als personenbezogene Daten angesehen werden können. Allerdings werden die IP-Adressen in vielen Fällen in aggregierter oder verschleierter Form verarbeitet und die Daten werden in Europa gehostet, um den datenschutzrechtlichen Anforderungen gerecht zu werden.

Bis zu welchem Grad lassen sich CDNs für dynamische Websiteinhalte nutzen und für welche Sites oder Anwendungen ist ein CDN nicht geeignet?

CDNs eignen sich hervorragend zur Beschleunigung und effizienten Bereitstellung von statischen Webseiteninhalten. Für stark dynamische Webseiteninhalte sind CDNs weniger geeignet, da das Caching von Inhalten problematisch sein kann. Dynamischer Content wird für den jeweiligen User generiert und andere User könnten dann „falschen" Content ausgeliefert bekommen. Das kann einerseits harmlos sein, wenn es sich nur um eine falsche Zeitzone handelt. Andererseits kann es auch gefährlich sein, wenn etwa Login-Seiten gecached werden. Auch durch einen sauberen Umgang mit HTTP-Headern wie zum Beispiel Cache Control können Webseiten mit dynamischem Content von einem CDN profitieren.

Wann ist die Migration von einem client-basierten CDN zu einem Cloud Computing Model sinnvoll? Welche Herausforderungen und Vorteile gehen damit einher?

Die Migration zu einem Serverless-Computing-Modell kann sinnvoll sein, wenn eine Webseite oder Anwendung sehr viel dynamischen Inhalt enthält und eine verbesserte Leistung und Skalierbarkeit erforderlich ist. Zu den Herausforderungen bei der Migration gehören die Komplexität der Konfiguration und Verwaltung sowie eine unterschiedliche Kostenstruktur.

Ein Content Delivery Network (CDN) bietet zahlreiche Vorteile für die Bereitstellung von Webinhalten, gleichzeitig sind damit auch spezifische Sicherheitsrisiken verbunden. Zu den wichtigsten Risiken gehören:

1. **DDoS-Angriffe:** Manche CDNs sind anfällig für Distributed Denial-of-Service-Angriffe (DDoS), bei denen eine große Anzahl von Anfragen gleichzeitig an das CDN gesendet wird, um die Ressourcen zu überlasten und die Dienste zu beeinträchtigen.
2. **Caching von bösartigen Inhalten:** Wenn es einem Angreifer gelingt, bösartige Inhalte in das CDN einzuschleusen, können diese über das Netzwerk verbreitet werden. Dadurch können Benutzer auf gefährliche Inhalte zugreifen und gefährdet werden.
3. **SSL/TLS-Schwachstellen:** CDNs können Sicherheitslücken in der SSL/TLS-Kommunikation aufweisen, insbesondere wenn die Verschlüsselung nicht ordnungsgemäß implementiert ist oder veraltete Protokolle verwendet werden.
4. **Datenlecks:** Konfigurationsfehler oder mangelnder Schutz sensibler Daten können zu Datenlecks führen, bei denen vertrauliche Informationen abgefangen oder kompromittiert werden können.
5. **Ausfall des CDN-Anbieters:** Wenn der CDN-Anbieter von einem Ausfall oder einem Sicherheitsvorfall betroffen ist, kann dies zu erheblichen Störungen für alle Kunden führen, die seine Dienste nutzen.

Darüber hinaus kann das CDN selbst als Teil eines Angriffes zweckentfremdet werden. Bei einem sogenannten Range-Amplification-Angriff (kurz Range Amp) werden speziell gestaltete Anfragen verwendet, um die grundlegende Funktion zu untergraben. Statt die Leistung zu verbessern und die Last auf Webservern zu verringern, wird das CDN in einen Angriffsverstärker verwandelt.

Der HTTP-Standard erlaubt HTTP Range Requests, mit denen ein Client (in der Regel ein Browser) einen bestimmten Teil (Byte-Bereich) einer Datei anfordern kann. Der Verwendungszweck ist das Anhalten/Wiederaufnehmen von Downloads oder das Wiederherstellen abgebrochener Anfragen.

Die Implementierung von Range Requests in CDN-Netzwerken funktioniert aus Sicht der Besucher wie erwartet. Hat jedoch das CDN diese Ressource nicht im Cache, gibt es verschiedene Aktionsmöglichkeiten: Entweder es wird die gesamte Ressource anfordern, damit sie für den nächsten Besucher aus dem Cache zur Verfügung steht, oder es wird den spezifischen Bereich anfordern und sich nicht die Mühe machen, einen Teil der Ressource zwischenzuspeichern.

Eine solche Range-Amp-Attacke ist am effektivsten, wenn sie auf CDNs angewendet wird, welche die gesamte Ressource abrufen. Erstellt der Angreifer exakt zugeschnittene Anfragen, kann die Funktion des CDNs missbraucht und in einen Angriffsverstärker umgewandelt werden.

Ein effektiver Range-Amp-Angriff:

1. Zielt auf eine große im CDN verfügbare Ressource ab.
2. Überzeugt das CDN, dass es eine neue Kopie vom Webserver des Opfers abrufen muss.
3. Fordert nur einen kleinen Byte-Bereich an

Kommen wiederholt aus verteilten Quellen solche Anfragen, wird das CDN nur sehr wenig Datenverkehr von außen sehen. Es sind lediglich ein paar kleine Anfragen, mit entsprechend kleinen Antworten von vielen verschiedenen IP-Adressen. Stattdessen kommt es zu einem deutlichen Anstieg des Datenverkehrs beim Opfer des Angriffes, also seinem direkten Client, der auf die Anfragen mit großen Dateien antwortet.

Das Ziel des Angriffs ist eine ungewöhnlich hohe Anzahl von Anfragen für eine große Ressource durch das CDN, die alle verfügbaren Ressourcen aufbraucht. Zwischen der Webseite und dem CDN besteht in der Regel eine vertrauensvolle Beziehung. Das bedeutet, dass der gesamte Datenverkehr zum/vom CDN auf der „Whitelist“ steht oder automatisch zugelassen wird. Dadurch ist das Opfer des Angriffs diesem nahezu schutzlos ausgeliefert. Wenn das CDN nicht auf einer solchen Whitelist steht, kann der plötzliche Anstieg des Datenverkehrs dazu führen, dass das Opfer aus Versehen den Datenverkehr vom CDN vorübergehend blockiert, so dass große Teile der Website nicht mehr verfügbar sind.

Die Implementierung eines Content Delivery Networks (CDN) bietet zahlreiche Performance-Vorteile wie eine verbesserte Ladezeit, geringere Latenz und reduzierte Datenübertragungskosten. Zudem können CDNs die Sicherheit erhöhen und Compliance-Anforderungen erfüllen. Um davon optimal zu profitieren, sollte auf einen zuverlässigen CDN-Anbieter zurückgegriffen werden, der sowohl umfassende Sicherheitslösungen bietet als auch die Einhaltung von Datenschutzbestimmungen sicherstellt.

Ein Blick auf die zukünftigen Entwicklungen zeigt, dass die Integration von generativer künstlicher Intelligenz (KI) eine entscheidende Rolle spielen wird. Während KI-gesteuerte Angriffe und Verteidigungsmechanismen zunehmend komplexer werden, besteht die Gefahr, dass die Kluft zwischen den am besten und den am schlechtesten gerüsteten Organisationen größer wird.

Unternehmen weltweit sollten sich dieser Herausforderung bewusstwerden und ihre Sicherheitsstrategien entsprechend anpassen. Durch eine ganzheitliche Herangehensweise, die sowohl technologische Innovationen als auch die menschliche Dimension der Cybersicherheit berücksichtigt. Es geht um den Aufbau eines ganzheitlichen Cybersicherheitsökosystems. Denn damit können Organisationen ihre Cyber-Resilienz stärken und sich wirksam gegen die zunehmenden Bedrohungen schützen.

Nachweise

1 https://www.weforum.org/agenda/2023/01/cybersecurity-storm-2023-experts-davos23/

2 https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2024-press.html

3 https://www.reuters.com/world/europe/russian-hacktivists-briefly-knock-german-websites-offline-2023-01-25/

4 https://cybernews.com/news/european-investment-bank-cyberattack-russia/

5 https://cybernews.com/security/microsoft-outlook-outage-anonymous-sudan/

6 https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement

7 https://www.reuters.com/technology/denmarks-central-bank-website-hit-by-cyberattack-2023-01-10/

8 https://www.reuters.com/technology/websites-several-german-airports-down-focus-news-outlet-2023-02-16/

9 https://www.csoonline.com/de/a/netzwerkangriff-auf-it-dienstleister-der-energieversorgung-filstal,3674523

10 https://edition.cnn.com/2023/04/21/business/eurocontrol-russia-hackers/index.html

11 https://therecord.media/hacker-group-anonymous-sudan-demands-three-million-from-sas

12 https://cybernews.com/news/european-investment-bank-cyberattack-russia/

13 DdoS attack on 12 Norway government websites - Cybersecurity Insiders (cybersecurity-insiders.com)

14 Russian hackers crash Italian bank websites, cyber agency says | Reuters

15 Wells Fargo banking services halted by Anonymous Sudan DDoS - Cyber Daily

16 Host of EU summit Spain target of DDoS cyberattacks | Reuters

17 ChatGPT Down As Anonymous Sudan Hackers Claim Responsibility (forbes.com)

18 Several websites of Belgian institutions disrupted yesterday by DDoS attack | Centre for Cyber security Belgium

19 BSI-Chefin: „Die Bedrohungslage ist so groß wie nie“ – Wirtschaft – SZ.de (sueddeutsche.de)

20 Inside the World of NoName057(16): Unmasking the Notorious DDoS Hackers | FalconFeeds

21 https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/

22 https://decoded.avast.io/martinchlumecky/bobik/

23 https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/fachberichte/Bericht-Analyse-DDoS-NCSC-DE.pdf.download.pdf/Bericht-Analyse-DDoS-NCSC-DE.pdf

24 https://securityboulevard.com/2024/01/datadome-recognized-in-forrester-landscape-Bot Management-q1-2024-report/

25 https://datadome.co/resources/us-bot-security-report/

26 https://www.juniperresearch.com/research/fintech-payments/fraud-identity/online-payment-fraud-research-report/

27 https://www.zdnet.com/article/newly-discovered-android-malware-has-infected-thousands-of-devices/

28 https://www.security-insider.de/bad-bots-ki-roboter-uebernehmen-internet-a-8620c7f12b55dd1db2e15e55b29a0c66/

29 https://www.heise.de/news/Sicherheitsluecken-Statistik-2023-gab-es-15-Prozent-mehr-CVEs-als-im-Vorjahr-9591523.html

Hauptsitz

Link11 Group
Lindleystr. 12
60314 Frankfurt