LINK11

DDOS-REPORT

1. Halbjahr 2023

www.link11.com

Inhalt

Einleitung und Zusammenfassung

Mehr DDoS-Angriffe: intelligenter, komplexer und intensiver

Zu Beginn des Jahres hat Sadie Creese, Professorin für Cybersicherheit an der Oxford-Universität, auf dem World Economic Forum[1] in Davos vor dem aufkommenden „Cybersturm“ gewarnt. Auch wenn sie im Januar 2023 nicht abschätzen konnte, wie heftig dieser ausfallen sollte, hat sie im Rückblick auf die ersten sechs Monate dieses Jahres Recht behalten.

Ransomware, Phishing und Distributed-Denial-of-Service-Angriffe (DDoS) gehören nach Einschätzungen nationaler und internationaler Behörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der Agentur der Europäischen Union für Cybersicherheit (ENISA) und dem Federal Bureau of Investigation (FBI) zu den größten Bedrohungen in der digitalen Landschaft, Tendenz steigend.

Das betrifft nicht nur die Anzahl der weltweit registrieren Cybervorfälle insgesamt, sondern auch die Komplexität der einzelnen Angriffe sowie die Unsicherheit auf Seiten der Unternehmen und Organisationen. Zunehmend kombinieren Cyberkriminelle verschiedene Angriffsarten. *Ransomware und DDoS-Angriffe sind beispielsweise eine solch verheerende Kombination.*

Die sogenannte „Triple Extortion“ sieht wie folgt aus: Die Angreifer drohen mit einem DDoS-Angriff, dann folgt ein Überlastungsangriff, in dessen Windschatten die Täter unbemerkt die Schadsoftware ins System einschleusen oder Daten abziehen. Im Anschluss an die Verschlüsselung durch die eingeschleuste Ransomware drohen sie entweder mit der Veröffentlichung der kopierten und analysierten Daten im Darknet oder veröffentlichen die gestohlenen Daten direkt. Dieser Trend wird durch die florierende „Cybercrime-as-a-Service“-Industrie zusätzlich verstärkt.

Die Konsequenzen für Unternehmen können enorm sein. Gestohlene oder veröffentlichte Kundendaten stellen eine existenzielle Bedrohung für die Reputation des Unternehmens dar, Kunden verlieren das Vertrauen. Solche Auswirkungen reichen weit über die rein finanziellen Schäden hinaus.

Neben der wachsenden „Cybercrime-as-a-Service“-Industrie spielt zusätzlich die rasante Zunahme von smarten IoT- und Cloud-Technologien den Kriminellen in die Karten. Botnetze haben sich zu einer der größten Triebkräfte für DDoS-Angriffe entwickelt. Weltweit sind täglich zwischen 500.000 und 1.000.000 IoT-Hosts und Cloud-Server-Instanzen aktiv. Diese erzeugen mehr als 40 % des gesamten DDoS-Traffics.[2] Die Täter können auf ein riesiges Arsenal an Botnetzen zugreifen, dass sie mit immer intelligenter werdenden Attacken optimal zu nutzen wissen.

Diese verstärkten Aktivitäten konnte auch das Link11 Security Operations Center (LSOC) in der ersten Jahreshälfte 2023 beobachten: Die Anzahl der im Link11-Netzwerk registrierten Attacken ist im ersten Halbjahr um mehr als 70 % gestiegen. Besonders von April bis Juni kam es zu deutlich mehr DDoS-Angriffen als noch im 2. Quartal 2022.

Auch der anhaltende Krieg zwischen Russland und der Ukraine hat einen weiteren Anstieg politisch motivierter DDoS-Angriffe durch wohlorganisierte Angreifer ausgelöst. Die prorussischen Hackergruppen „REvil“, „Killnet“ und die seit Anfang des Jahres agierende neue Gruppe „Anonymous Sudan“ haben sich sogar zu einem Hacker-Kollektiv, dem sogenannten „Darknet Parliament“[3], zusammengeschlossen, um ihre Schlagkraft weiter zu erhöhen.

Die „Hacktivisten“ haben weltweit mit ihren politisch motivierten DDoS-Angriffen für mehr als nur mediale Aufmerksamkeit gesorgt. Zu den bekanntesten Opfern gehören zahlreiche deutsche Bundesländer und Behörden[4], die europäische Investitionsbank[5] und Microsoft[6].

Auch wenn es bisher zu keinen größeren Ausfällen gekommen ist, sollten die politisch motivierten DDoS-Attacken nicht unterschätzt werden. Denn anders als bei den überwiegend finanziell motivierten Angriffen stehen ideologische Motive und damit auch andere Ziele im Vordergrund.

Besonders gefährdet sind kritische Infrastrukturen (KRITIS). Durch ihre herausragende Bedeutung für Wirtschaft und Gesellschaft stehen sie vermehrt im *Fadenkreuz von Cyberkriminellen*. Ein erfolgreicher Angriff auf kritische Infrastrukturen kann erhebliche gesellschaftliche, wirtschaftliche sowie politische Folgen haben.

Nicht nur die Anzahl der DDoS-Angriffe hat im Betrachtungszeitraum deutlich zugenommen, sondern auch die Intensität der Attacken ist gestiegen. Besonders Hochvolumen-Angriffe haben in den ersten sechs Monaten signifikant zugenommen. Die vom LSOC gemessenen Bandbreiten überschritten jeden Monat die Marke von 200 Gbps. Der durchschnittliche Bandbreiten-Peak lag bei 454 Gbps, die größte Attacke wurde bei 795 Gbps gestoppt. Im 1. Halbjahr 2022 war die größte Attacke 574 Gbps groß.

Während die Intensität der Angriffe im ersten Halbjahr verglichen mit dem Vorjahreszeitraum zugenommen hat, ist die durchschnittliche Angriffsdauer im Vergleich zur ersten Jahreshälfte 2022 gesunken. Sobald die beabsichtigten Ergebnisse nicht erreicht werden können, werden die DDoS-Attacken frühzeitig abgebrochen.

Es scheint, dass die Angreifer zunehmend künstliche Intelligenz nutzen, um ihre Methoden und Angriffstypen zu verbessern. Ende März 2023 hat Europol, die Strafverfolgungsbehörde der Europäischen Union, ihren jüngsten Bericht über „ChatGPT“ mit dem Titel „The Impact of Large Language Models on Law Enforcement“ veröffentlicht.[7] Darin warnt Europol vor dem möglichen kriminellen Missbrauch von Chatbots wie ChatGPT, die auf künstlicher Intelligenz (KI) basieren.

Neben dem Trend zu kürzeren Angriffen erreichen die im Link11-Netzwerk beobachteten DDoS-Angriffe im ersten Halbjahr 2023 im Durchschnitt bereits nach 60 Sekunden ein kritisches Volumen, verglichen mit dem Durchschnitt von 93 Sekunden im Vergleichszeitraum 2022.

Demgegenüber zeigt sich bei den langanhaltenden Attacken ein anderes Bild: Die längste Attacke im ersten Halbjahr 2023 war 1.444 Minuten lang, das entspricht 24 Stunden und 4 Minuten. Der längste DDoS-Angriff in der ersten Jahreshälfte 2022 betrug lediglich 981 Minuten, das entspricht knapp 16,5 Stunden.

Was die Multi-Vektor-Angriffe betrifft, zeigt sich die größte Veränderung bei HTTPS-Attacken. Ihr Anteil ist auf 30 % gestiegen, was einen deutlichen Anstieg an Layer-7-Angriffen erkennen lässt. Die Abwehr verschiedener Angriffsvektoren stellt für jede Schutzlösung eine Herausforderung dar, die die Time-to-Mitigate (TTM) verlangsamen kann.

Zuverlässig schützen nur DDoS-Lösungen, die immer auf dem neusten Stand sind, was die Angriffsmethoden angeht. Nur so können sie mit der sich ständig wandelnden Bedrohungslandschaft Schritt halten. Selbst ein einzelner gezielter Angriffsvektor kann großen Schaden anrichten, wenn die IT-Sicherheit nicht auf dem neuesten Stand ist.

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.[8]

Januar 2023

Russische „Hacktivisten" legen deutsche Websites lahm

Als Reaktion auf die Entscheidung Berlins, Panzer in die Ukraine zu schicken, haben russische Hacker-Aktivisten am 25. Januar mehrere deutsche Websites offline geschaltet.[9]

Januar 2023

Russische Cyberbande nimmt US-Krankenhäuser ins Visier

Als Reaktion auf Bidens Versprechen Dutzende von Militärpanzern an die Ukraine zu liefern, hat es Killnet auf mindestens 14 US-Gesundheitseinrichtungen abgesehen.[10]

Februar 2023

Mehrere deutsche Flughäfen von DDoS-Angriffen betroffen

Die Websites von sieben deutschen Flughäfen wurden von DDoS-Attacken getroffen und waren nicht erreichbar.[11]

Februar 2023

Dänische Krankenhäuser Ziel von DDoS-Angriffen

Anonymous Sudan hat neun Krankenhäuser in Dänemark mit DDoS-Attacken angegriffen und deren Websites für mehrere Stunden lahmgelegt.[12]

Februar 2023

Tor- und I2P-Netzwerke massiv eingeschränkt

Eine Welle von DDoS-Angriffen greift das Netzwerk immer wieder seit mindestens Juli 2022, sodass die Nutzer keine Seiten laden oder auf Dienste zugreifen konnten.[13]

März 2023

Düsseldorfer Rüstungskonzern Rheinmetall von Hackern angegriffen

Der Rüstungskonzern Rheinmetall aus Düsseldorf hat am Dienstag eine Cyberattacke weitgehend abwehren können.[14]

Marz 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 Webseiten-Performance deutlich einschränkt.[15]

Marz 2023

Prorussische Hackergruppe NoName057(16) greift französische Parlamentsseite an

NoName057(16) hat die Website der französischen Nationalversammlung für mehrere Stunden lahmgelegt, um eine Botschaft an den französischen Präsidenten Emmanuel Macron zu senden.[16]

April 2023

Angriffe auf offizielle Websites

Auf mehrere offizielle Internetauftritte von Bund und Ländern sind Cyberangriffe verübt worden. Teilweise konnten die Attacken abgewehrt werden.[17]

April 2023

Cyberangriff auf kanadischen Stromversorger

Eine prorussische Hackergruppe hat sich zu einem Cyberangriff auf den staatlichen Stromversorger von Québec bekannt. Infolgedessen gingen die Website, die App und die Info-Panne-Website von Hydro-Québec zur Überprüfung von Stromausfällen offline.[18]

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.[19]

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.[20]

Mai 2023

DDoS-Angriffe auf polnische Nachrichtenagenturen

Mehrere Nachrichtenagenturen meldeten auf Twitter, dass sie von DDoS-Angriffen betroffen sind, darunter die Tageszeitung Gazeta Wyborcza und die Online-Nachrichtenseite.[21]

Mai 2023

NoName057 hat verschiedene isländische Websites angegriffen

Im Vorfeld des Gipfeltreffens des Europarats gab es verstärkte DDoS-Angriffe auf die isländische Infrastruktur.[22]

Juni 2023

Microsoft Outlook nach Hackerangriffen außer Betrieb

Microsoft Outlook war am Montag für Tausende von amerikanischen Nutzern nicht erreichbar. Anonymous Sudan deklarierte eine Kampagne gegen US-Unternehmen und -Infrastruktur.[23]

Juni 2023

Schweizer Regierung und Bundesbahnen von Cyberangriffen betroffen

Mehrere Websites der Bundesverwaltung sind von einem DDoS-Angriff getroffen worden.[24]

Juni 2023

DDoS-Angriff auf die Europäische Investitionsbank

Prorussische Hacktivisten haben europäische Bankinstitute angegriffen und die Europäische Investitionsbank (EIB) als eines ihrer Opfer genannt.[25]

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 ersten Halbjahr 2023 wieder deutlich gestiegen. Von Januar bis Ende Juni 2023 stieg die Anzahl der DDoS-Angriffe im Vergleich zum Vorjahreszeitraum um mehr als 70 %. Mit dem Anstieg der Anzahl insgesamt ist auch die Zunahme täglicher Attacken verbunden. Besonders im 2. Quartal 2023 kam es zu deutlich mehr DDoS-Angriffen als noch im Vergleichszeitraum.

Der anhaltende Krieg zwischen Russland und der Ukraine hat einen weiteren Anstieg politisch motivierter DDoS-Angriffe durch wohlorganisierte Angreifer ausgelöst. Zu den prominenten Akteuren zählen die prorussische Gruppe Killnet, NoName057(16) und Anonymous Sudan. Ihnen gemeinsam ist, dass *DDoS-Attacken von ihnen als bevorzugtes Mittel* der ideologisch motivierten Cyberangriffe eingesetzt werden. Weltweit nehmen die geopolitischen Spannungen zu, sodass die Bedrohung solcher Angriffe zunehmend wächst.

Diese DDoS-Attacken zielen auf kritische Infrastrukturen (KRITIS), öffentliche Einrichtungen und politische Organisationen ab. Die prorussischen Hackergruppen haben bereits im vergangenen Jahr den Cyberkrieg ausgerufen.[26] Ihr Ziel ist es, die Moral der Bevölkerung zu schwächen und größtmöglichen Schaden anzurichten, wie Microsoft im Bericht „Defending Ukraine: Early Lessons from the Cyber War“ aufgezeigt hat.[27]

Deutschland, Dänemark, Polen und die Schweiz haben in diesem Jahr die Auswirkungen dieser Erklärung deutlich gespürt. 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.[28]

Im ersten Halbjahr 2023 haben die DDoS-Aktivitäten im Rahmen des patriotischen Hacktivismus im Vergleich zum Vorjahreszeitraum einen beunruhigenden Höhepunkt erreicht. Das Bedrohungspotenzial politisch motivierter Cyberangriffe wächst 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.

Auffällig ist auch, dass sich mehrere prorussische Hacktivistengruppen wie Killnet, Anonymous Sudan, REvil oder NoName057(16) an den Angriffen beteiligen und sich in neuen Hacker-Kollektiven zusammenschließen. Neue Akteure wie Anonymous Sudan sind zudem noch unberechenbar, was eine weitere Eskalation der Angriffe zur Folge haben könnte.

Cyberkriminelle und staatliche Akteure nutzen DDoS-Angriffe als wirksames Mittel, um politischen Druck auszuüben, kritische Systeme zu sabotieren oder Lösegeld zu erpressen. Derzeit ist keine Organisation vor politisch motivierten Cyberangriffen sicher. Es werden gezielt Websites westlicher Länder ins Visier genommen.

Angesichts dieser vielfältigen Bedrohungen ist der Schutz vor DDoS-Angriffen von entscheidender Bedeutung, um die Stabilität und Sicherheit unserer Gesellschaft aufrechtzuerhalten. Es bedarf einer koordinierten und umfassenden Abwehrstrategie, um die Resilienz unserer kritischen Infrastrukturen zu stärken und potenzielle Angreifer abzuschrecken. Mehr dazu finden Sie im Link11-Whitepaper: *Kritische Infrastrukturen im Fadenkreuz.*

„Es ist offensichtlich, dass der Schutz vor Cyberangriffen eine immer größere Herausforderung darstellt, um Sicherheit in unserer vernetzten Welt zu gewährleisten. Umso wichtiger ist eine effektive IT-Sicherheitsstrategie, die auf Automatisierung und Geschwindigkeit setzt. In fast jeder Situation, in der ein DDoS-Angriff gefährlich sein kann, haben wir in der ersten Jahreshälfte eine Zunahme festgestellt."

Jens-Philipp Jung, Geschäftsführer, Link11

Anonymous Sudan – wer steckt dahinter?

Im Januar 2023 sind neue Angreifer auf der globalen Bühne erschienen: Anonymous Sudan. Seitdem hat die Hackergruppe weltweit eine Reihe von DDoS-Angriffen gegen Länder, Unternehmen und Regierungseinrichtungen durchgeführt. Dabei haben sie besonders kritische Infrastrukturen ins Visier genommen, darunter Finanzinstitute, Luftfahrtunternehmen, Einrichtungen im Gesundheitswesen sowie Regierungswebsites.

Betroffen waren im ersten Halbjahr 2023 unter anderen Schweden, Dänemark und die Niederlande sowie Australien und Israel. Zu weitreichenden Flugunterbrechungen führte der Angriff auf die Website und die mobile App von Scandinavian Airlines (SAS). Auch bei Microsoft sorgten die DDoS-Attacken von Anonymous Sudan für Ausfälle und Unterbrechungen bei mehreren Produkten und Diensten wie zum Beispiel Teams und Outlook.

Es scheint mehrere Verbindungen zu prorussischen Hackergruppen wie Killnet und anderen Cyberkriminellen zu geben. Erst im Juni 2023 hat Anonymous Sudan angekündigt, gemeinsam mit Killnet und REvil als Hacker-Kollektiv „Dark Parliament" einen „massiven Angriff" auf europäische und US-amerikanische Finanzinstitute durchzuführen.[29] Letztlich wurde die Europäische Investitionsbank angegriffen.

Trotz des Namens hat Anonymous Sudan keine tatsächliche Verbindung zum Sudan oder der früheren Anonymous-Gruppe, die dort aktiv war. Viele Sicherheitsforschende[30] sind sich einig, dass Anonymous Sudan von Russland staatlich gesponsert wird.[31] Es gibt einige Indizien, die darauf hinweisen, dass es sich um russische Akteure handelt, die sich als sudanesische Personen mit islamistischen Motiven ausgeben.

Zum Beispiel postete die Gruppe ursprünglich nur auf Russisch oder Englisch. Als Beobachter die Herkunft der Hacker in Frage stellten, haben sie begonnen auf Arabisch zu kommunizieren. Diese Tarnung ermöglicht es ihnen, westliche Ziele unter dem Deckmantel des Hacktivismus ins Visier zu nehmen.

Anonymous Sudan nutzt bei den DDoS-Angriffen verschiedene Taktiken, darunter HTTP(S)-Flood-Angriffe, Cache-Umgehungsversuche und Slow Loris-Techniken.[32] Die Angriffe von Anonymous Sudan lassen auf eine gut finanzierte und ausgeklügelte Operation schließen. Die Gruppe verwendet bezahlte Proxy-Server und eine Cloud-Infrastruktur, was sie von herkömmlichen Hacktivistengruppen unterscheidet. Die Abwehr ihrer Angriffe erfordert robuste DDoS-Schutzstrategien, die den Einsatz von bezahlten Proxy-Diensten berücksichtigen und Angriffe auf der Anwendungsebene wirksam bekämpfen können.

Es bleibt abzuwarten, wie sich die Situation entwickelt und welche Ziele Anonymous Sudan als Nächstes ins Visier nehmen wird. Die internationale Gemeinschaft und Unternehmen müssen wachsam sein und geeignete Maßnahmen ergreifen, um ihre digitalen Infrastrukturen vor diesen Cyberangriffen zu schützen.

Entwicklung des „Onsets“

Eine neue Ära – smarte Turboattacken

Bei den im Link11-Netzwerk registrierten DDoS-Attacken wird seit dem ersten Halbjahr 2022 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 ersten Halbjahr 2023 erreichen DDoS-Angriffe im Durchschnitt bereits nach 60 Sekunden ein kritisches Niveau. Verglichen mit dem Durchschnitt von 93 Sekunden im Vergleichszeitraum von Januar bis Ende Juni 2022 erreichen diese „Turboangriffe“ deutlich schneller ein kritisches Volumen.

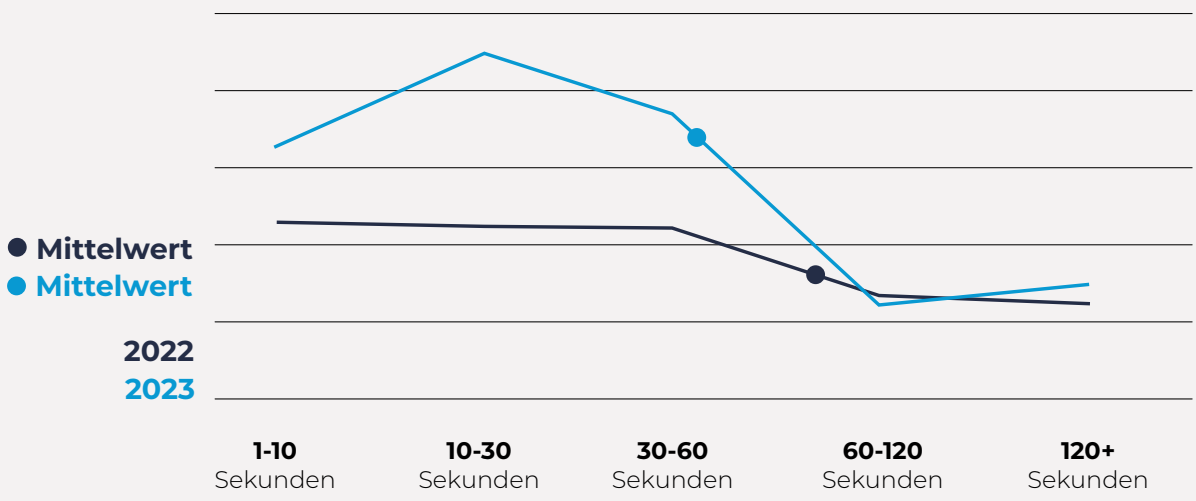
Ein Blick auf die Verteilung der Zeit, die während des DDoS-Angriffes bis zum Erreichen des Höhepunktes vergeht, zeigt für das erste Halbjahr 2023 folgende Ergebnisse: In knapp einem Viertel der Angriffe (24 %) wurde innerhalb der ersten zehn Sekunden die kritische Nutzlast erreicht. Im ersten Halbjahr 2022 lag dieser Anteil ebenfalls bei 24 %.

In der ersten Jahreshälfte 2023 machten Angriffe, die in zehn bis 30 Sekunden ihren Maximalwert erzielten, rund ein Drittel aller im Netzwerk registrierten Attacken aus (32 %). Im Vergleich dazu näherten sich ein Viertel der Angriffe (24 %) im 1. Halbjahr 2022 in der gleichen Zeit ihrem Höhepunkt.

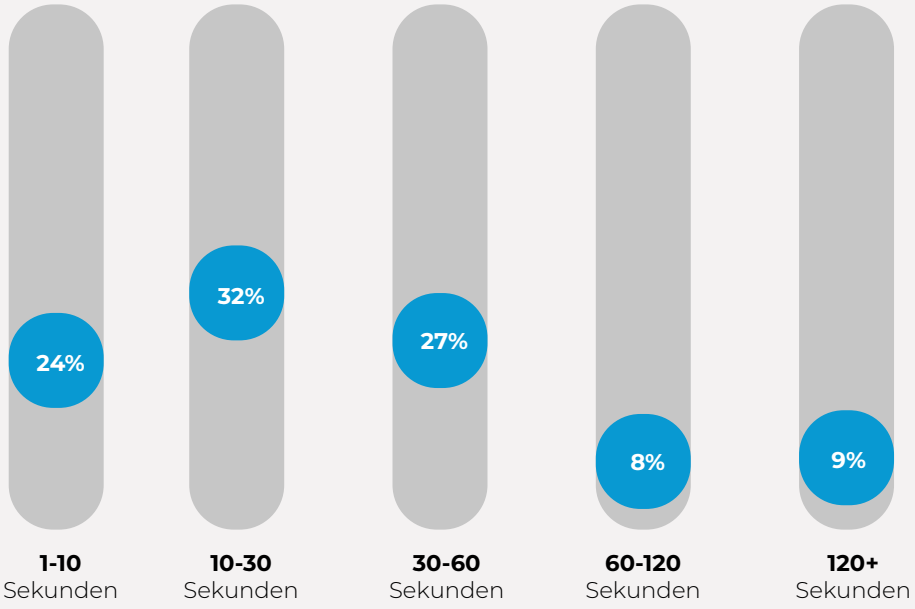
In etwas mehr als einem Viertel der Fälle (27 %) dauerte es bei den DDoS-Angriffen im ersten Halbjahr 2023 zwischen 30 und 60 Sekunden, bis der kritische Maximalwert erreicht wurde. Dieser Wert lag im Vorjahreszeitraum bei weniger als einem Viertel (24 %).

Bei 8 % der Angriffe wurde mehr als eine Minute Angriffszeit gemessen und nur bei rund jedem zehnten Angriff (9 %) der vom LSOC verzeichneten DDoS-Attacken dauerte es mehr als zwei Minuten, bis das kritische Niveau erreicht wurde. In der ersten Jahreshälfte 2022 erreichten 15 % der Angriffe in ein bis zwei Minuten ihren Höhepunkt und in 13 % der Fälle dauerte es mehr als zwei Minuten.

Dauer bis zum Höhepunkt einer Attacke I 1. Halbjahr 2023 vs. 1. Halbjahr 2022



Verteilung der Dauer bis zum Höhepunkt der Attacke



Im Angriffsfall ist es entscheidend, dass keine wertvolle Zeit bei der manuellen Bewertung von Vorfällen oder beim reaktiven Umschalten des Datenverkehrs und der Routing-Änderungen verstreicht. Zusätzlich können unerwartete Routing-Probleme oder komplexere Angriffsmethoden zu weiteren Verzögerungen in der Abwehr führen, die erhebliche Schäden verursachen können.

Um das Netzwerk effektiv zu schützen, sollte der Datenverkehr in Echtzeit mit smarten, schnellen und sicheren Methoden analysiert werden, um maximale Transparenz über den gesamten Netzverkehr zu gewährleisten. Bei einer effizienten IT-Sicherheitsstrategie ist die Mischung aus einem Basis-Schutz sowie intelligenter und automatisierter KI-Technologie eine effektive Methode, um DDoS-Angriffe abzuwehren.

„Onset ist ein Maß dafür, wie schnell ein Angriff sein kritisches Volumen erreicht. Das Initiieren von DDoS-Angriffen über Tausende von Systemen hinweg erfordert eine gute Koordination und Organisation. Deshalb haben Angriffe normalerweise eine Anlaufzeit, bevor sie ihr volles Potenzial erreichen. Je schneller die kritische Nutzlast erreicht ist, desto professioneller und koordinierter war der Angriff. Für potenzielle Angriffsziele ist der Onset ein Hinweis darauf, wie viel Zeit sie haben, um ihre Verteidigung zu mobilisieren.“

Jag Bains, Vice President Solution Engineering, Link11

Entwicklung der Angriffsdauer

Angriffseffizienz dank intelligenter DDoS-Attacken

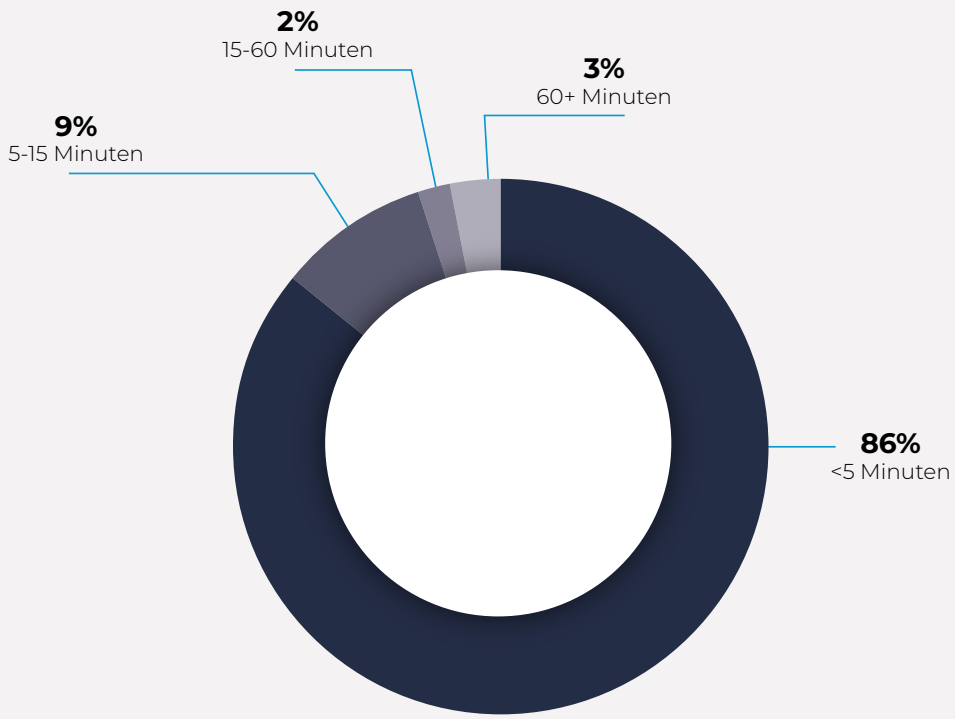
Die Dauer der im ersten Halbjahr 2023 im Link11-Netzwerk registrierten DDoS-Angriffe zeigt im Vergleich zum Vorjahreszeitraum unterschiedliche Entwicklungen. Der Trend zu kürzeren Angriffen hat sich bereits im Vorjahreszeitraum abgezeichnet. Die durchschnittliche Angriffszeit ist im Vergleich zur ersten Jahreshälfte 2022 weiter gesunken. Dies lässt sich darauf zurückführen, dass viele Angriffe in den ersten zwei Minuten abgebrochen wurden.

Es liegt nahe, dass die Angreifer immer smartere Angriffsmethoden einsetzen und einen Angriff frühzeitig abbrechen, wenn die beabsichtigten Ergebnisse nicht erzielt werden. Prallen die Angriffe zudem an gut geschützten Infrastrukturen ab, ziehen sich die Angreifer meist zurück, um ihre Ressourcen zu schonen und sie gegebenenfalls an anderer Stelle einzusetzen. Doch wenn es ihnen darum geht, die Ziele dauerhaft zu beeinträchtigen und erfolgreich Schäden zu verursachen, greifen sie zu langanhaltenden Attacken.

Bei den langanhaltenden DDoS-Angriffen zeigt sich, dass die jeweils längsten Attacken deutlich voneinander abweichen. Die längste Attacke im ersten Halbjahr 2023 war 1.444 Minuten lang, das entspricht 24 Stunden und 4 Minuten. Der längste DDoS-Angriff in der ersten Jahreshälfte 2022 betrug lediglich 981 Minuten, das entspricht knapp 16,5 Stunden.

Die weitere Analyse zeigt, dass die Länge der Angriffe zwischen wenigen Minuten und mehreren Stunden schwankte. Der Großteil der Angriffe (86 %) dauerte weniger als 5 Minuten. Ein Zehntel aller registrierten Angriffe (9 %) war zwischen 5 und 15 Minuten lang, nur zwei Prozent war zwischen 15 und 60 Minuten lang. Lediglich rund 3 % der Angriffe waren länger als 60 Minuten.

Angriffsdauer 1. Halbjahr 2023



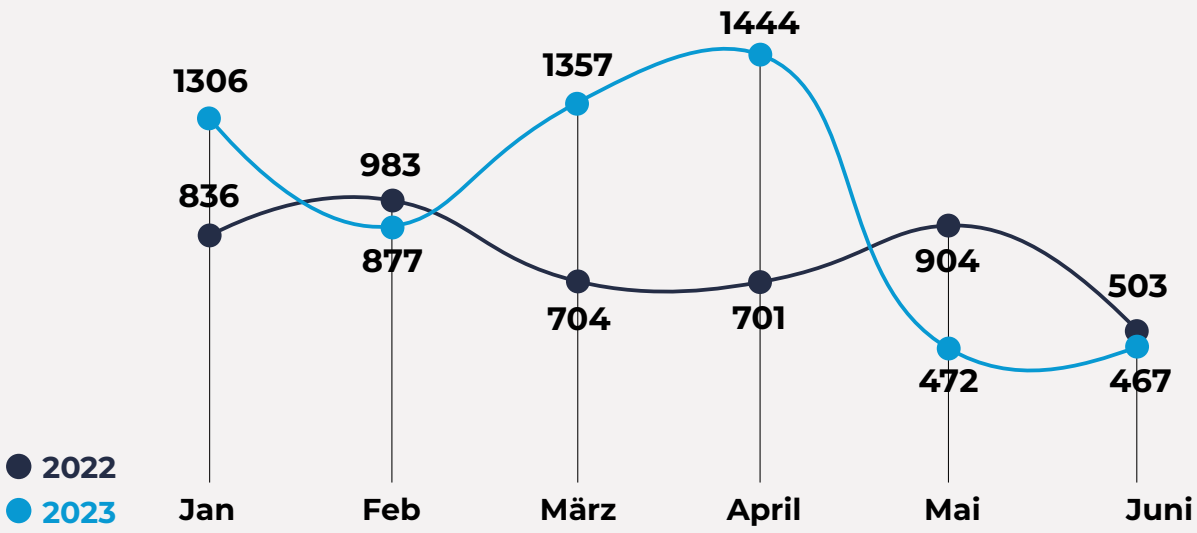
In der Verteilung der Angriffsdauer zeigt sich, wie wandlungsfähig die Angriffslandschaft ist. Die Taktiken, die Angreifer wählen, variieren je nach Angriffstechnik und Zielsetzung. Einerseits setzen sie auf „Blitzangriffe“, bei denen sie mit sehr großer Geschwindigkeit einzelne IP-Adressen der IT-Infrastruktur ihres Ziels nach Schwachstellen absuchen.

Andererseits nutzen sie kleine, aber hochfrequente DDoS-Attacken als Tarnung, während sie parallel dazu Server und Netzwerke ins Visier nehmen. In diesem Grundrauschen versteckt können die Cyberkriminellen unbemerkt durch die Hintertür ins System eindringen.

Eine weitere Möglichkeit für eine kürzere Dauer können auch intelligentere Angriffe sein. Die meisten Angriffe, die in der Lage sind, Vektoren innerhalb des Angriffes zu rotieren, verfügen über eine gewisse Erkennungsfunktion. Das heißt sie können feststellen, ob ein oder mehrere Vektoren erfolgreich sind. Folglich wird der Angriff abgebrochen, sobald er das Ziel mit keinem der zur Verfügung stehenden Vektoren mehr erreichen kann.

Um eine DDoS-Attacke erfolgreich abzuwehren, müssen die vorhandenen IT-Ressourcen in kürzester Zeit mobilisiert werden. Die schnelle Reaktion auf die Attacke ist dabei entscheidend, um Systemausfälle und weitere Schäden zu minimieren. Mit unvorhersehbaren Attacken stiften Angreifer Chaos und überfordern viele Sicherheitssysteme. Eine effektive Abwehr erfordert daher ein Höchstmaß an Präzision und Geschwindigkeit, um die IT-Infrastruktur effizient zu schützen.

Angriffsdauer in Minuten I 1. Halbjahr 2023 vs. 1. Halbjahr 2022



Entwicklung der Angriffsbandbreiten

Intensität der DDoS-Attacken gestiegen

Im ersten Halbjahr 2023 haben Hochvolumen-Attacken signifikant zugenommen. In den vergangenen sechs Monaten lag der durchschnittliche Bandbreiten-Peak bei 454 Gbps, während im ersten Halbjahr 2022 der Bandbreiten-Peak im Durchschnitt 325 Gbps betrug. Die vom LSOC gemessenen Bandbreiten überschritten jeden Monat die Marke von 200 Gbps. Die Intensität der DDoS-Angriffe hat im Betrachtungszeitraum gegenüber dem Vergleichszeitraum weiter zugenommen. Die größte Attacke wurde bei 795 Gbps gestoppt.

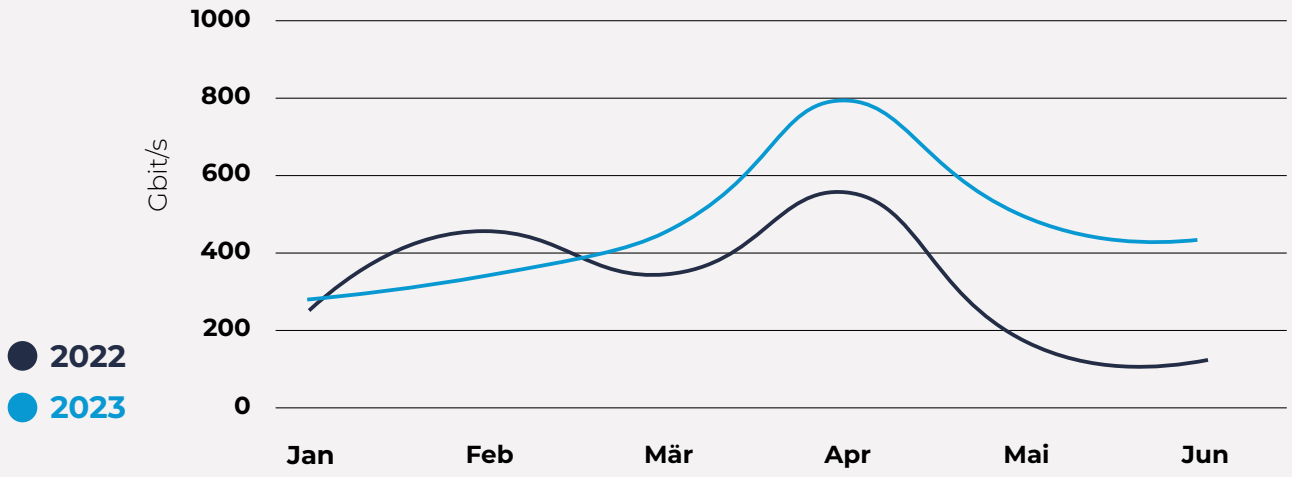
Die Zunahme des Angriffsvolumens ist besonders auf die Verbreitung von IoT-Geräten und den Zugriff von Cyberkriminellen auf mehr ungesicherte Rechenleistung und Kapazität in Hosting- und öffentlichen Clouds zurückzuführen. Täglich sind zwischen 500.000 und 1.000.000 weltweit verteilte IoT-Hosts oder Cloud-Server-Instanzen aktiv. Damit werden mehr als 40 % des gesamten DDoS-Verkehrs erzeugt [33].

Erst im Februar 2023 haben Sicherheitsforscher eine neue Variante der Mirai-Malware entdeckt.[34] Die Malware mit dem Namen „V3G4“ hat es besonders auf linuxbasierte Server und IoT-Geräte abgesehen. Die Entwickler der Schadsoftware sollen DDoS-Dienste an Cyberkriminelle verkaufen, damit Websites und Onlinedienste über dieses Botnetz angegriffen werden können.

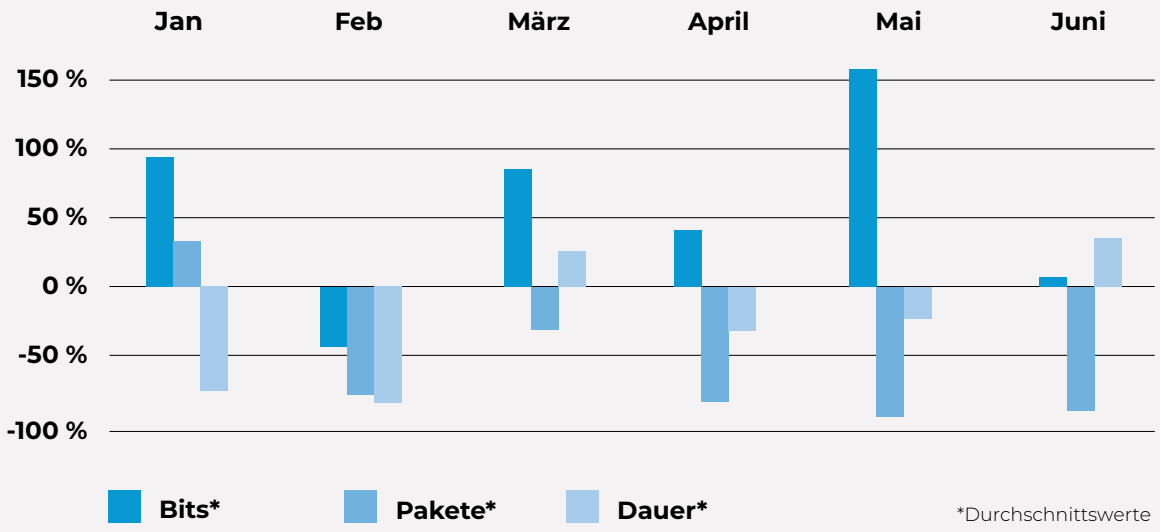
Im ersten Halbjahr wurde mit mehr als 168 Millionen Pakete pro Sekunde die größte bisher im Link11-Netzwerk registrierte Paketrate beobachtet. Die durchschnittliche Paketrate im Betrachtungszeitraum lag bei 413.000 Paketen pro Sekunde, der Durchschnitt der Anzahl im ersten Halbjahr 2022 war deutlich höher. Im Angriffsfall wurden durchschnittlich 1,4 Millionen Pakete pro Sekunde übermittelt.

Wirft man einen Blick auf die Korrelation zwischen Dauer und Intensität der DDoS-Angriffe, ist aktuell Folgendes erkennbar: Das LSOC konnte längere und kürzere Angriffe aller Intensitäten feststellen. Die durchschnittliche Dauer ist insgesamt gesunken, gleichzeitig ist das Gesamtvolumen der Angriffe deutlich gestiegen.

Bandbreiten-Peak pro Monat I 1. Halbjahr 2023 vs. 1. Halbjahr 2022



Veränderung der Dauer und Intensität der Attacken 1. Halbjahr 2023



Es gibt viele Angriffe, die so konzipiert sind, dass sie eine gefährliche Nutzlast aufweisen, ohne dass sie von herkömmlichen Schutzmaßnahmen erkannt werden. Ein „Layer-7-Slow-Post-Angriff“ kann etwa die Ressourcen eines Webservers vollständig aufbrauchen, indem er viele Anfragen mit jeweils 1 Byte pro Minute eintrudeln lässt, deren Summe weit unter den typischen Angriffsschwellenwerten liegt.

Slow-Post-Angriff

Es gibt eine begrenzte Anzahl von Ports, die auf einem Server verwendet werden können. Mit einem Slow-Post-Angriff wird versucht, alle verfügbaren Ports mit minimaler Bandbreite zu belegen. Beim Slow-Post-Angriff werden viele Verbindungen zu einem Webserver geöffnet. Jede Verbindung sendet eine POST-Anfrage (POST ist eine HTTP-Methode wie GET), aber die Übertragungsrate wird auf ein Minimum reduziert, damit der Port weiterhin genutzt wird. Dadurch werden alle verfügbaren Ports beansprucht, sodass keiner mehr frei ist, um legitime Anfragen zu empfangen.

Ähnlich verteilen „Carpet Bombing“-Angriffe ihre Bandbreite auf jede IP in einem Netzblock. Dadurch hat keine einzelne IP ein verdächtiges Datenverkehrsaufkommen. Anstatt auf eine einzige IP-Adresse zu zielen, verteilen die Angreifer den Angriff auf eine Reihe von IPs innerhalb desselben Netzwerks mit Hunderten oder Tausenden Adressen, was für unzureichend geschützte Hosting- und Cloud-Anbieter fast unmöglich zu entschärfen ist.

Oftmals erkennen Schutzlösungen diesen Traffic nicht als Anomalie. Stattdessen erfordert die Erkennung dieser Angriffe intelligentere Erkennungsmethoden als die herkömmliche Schwellenwertberechnung.

Je konzentrierter, gezielter und anspruchsvoller die DDoS-Angriffe werden, desto entscheidender sind Präzision und Geschwindigkeit bei der Erkennung und Abwehr. Besonders bei den schnell auftretenden und intensiven Attacken mit hoher Bandbreite und Paketraten geraten Schutzlösungen an ihre Grenzen. On-Premise-Lösungen können einfache und unkoordinierte Angriffe abwehren, aber komplexere und besonders intensive Angriffe sind in Lage, lokale Geräte zu überfordern.

Das bedeutet, dass im Umgang mit DDoS-Angriffen Zeit ein wesentlicher Faktor ist. Moderne On-Premise-Systeme nutzen oft hybride Cloud-Lösungen, die den Datenverkehr umleiten können, sobald er ein kritisches Niveau erreicht. Unter Laborbedingungen erfolgt diese Umleitung innerhalb von 10 bis 90 Sekunden, aber unter dem tatsächlichen Beschuss eines DDoS-Angriffes entsprechen Laborbedingungen nicht der tatsächlichen Realität.

Dabei ist entscheidend, wie viel Zeit bis zur ersten Reaktion auf den Angriff und dem Start der Schadensbegrenzung, der sogenannten Time-to-Mitigate (TTM), vergeht und wie lange es dauert, bis der Ursprungszustand wiederhergestellt wurde, die sogenannte Mean-Time-to-Repair (MTTR). Wie Link11 und andere Wettbewerber zu diesem entscheidenden Faktor positioniert sind, finden Sie in der Frost & Sullivan-Studie *„The New Benchmark: Why Fast DDoS Detection Is No Longer Good Enough“.*

„Zeit ist im Angriffsfall entscheidend – jede Sekunde zählt bei manuellen Bewertungen, Routing-Problemen und überlisteten Abwehrmechanismen. Eine schnelle TTM ist für eine effiziente Abwehrstrategie unverzichtbar. Ein hybrides System kann hier zum Einsatz kommen – aber nur, wenn es regelmäßig überprüft wird und immer auf dem neuesten Stand ist.“

Jag Bains, Vice President Solution Engineering, Link11

Multi-Vektor-Attacken

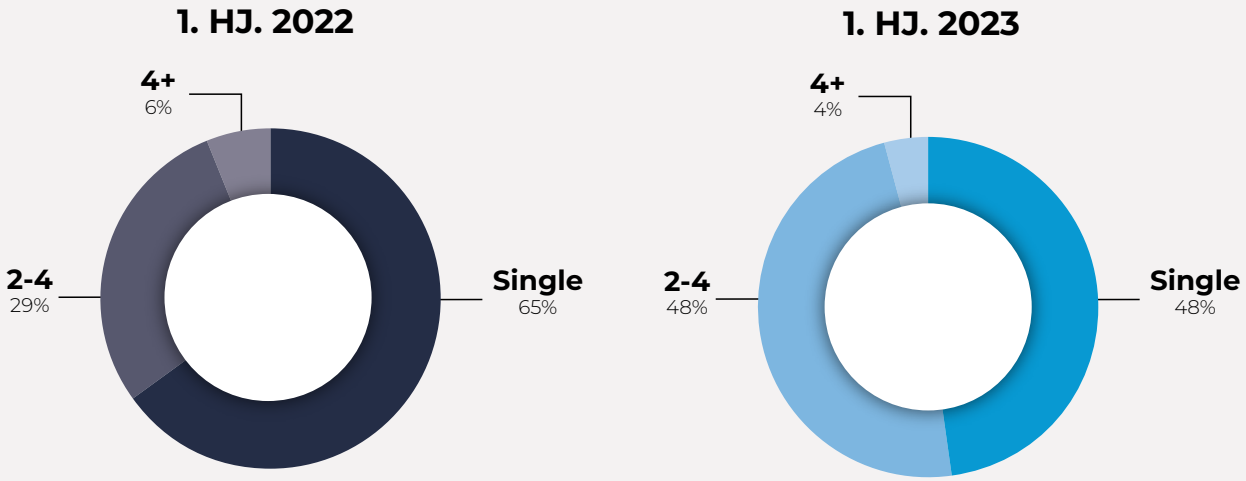
Verstärkt Multi-Vektor-Angriffe mit rotierenden Angriffsvektoren

Multi-Vektor-Attacken sind eine besonders gefährliche Art von DDoS-Angriffen. Im Gegensatz zu herkömmlichen Attacken, die nur einen Angriffsvektor nutzen, zielen Multi-Vektor-Angriffe gleichzeitig auf mehrere Schwachstellen in den Bereichen Transport, Applikation und Protokoll ab. Eine größere Anzahl von Vektoren macht es für die Verteidigungssysteme schwieriger, den Angriff zu erkennen und abzuwehren.

Die Kombination mehrerer Techniken steigert somit die Erfolgswahrscheinlichkeit für Angreifer, da viele Schutzlösungen nicht auf dem neuesten Stand sind. Die Angreifer starten ihren Übergriff mit mehreren Vektoren in der Hoffnung, dass zumindest einer der Vektoren durchkommt. Je mehr Vektoren dabei zum Einsatz kommen, desto größer ist die Wahrscheinlichkeit, dass ein oder mehrere Angriffe die Schutzmaßnahmen durchbrechen.

Aktuell kommen dabei innerhalb kürzester Zeit während einer DDoS-Attacke verschiedene Angriffsvektoren zum Einsatz. Diese können aufgrund falscher Identifizierung oder einer Lücke in den Sicherheitsmaßnahmen erfolgreich das IT-System oder einen Onlinedienst lahmlegen. Es ist daher wichtig, DDoS-Schutzlösungen zu nutzen, die effektiv gegen Multi-Vektor-Attacken auf allen Filterebenen arbeiten.

Anzahl der Single- und Multi-Vektor-Angriffe I 1. Halbjahr 2023 vs. 1. Halbjahr 2022

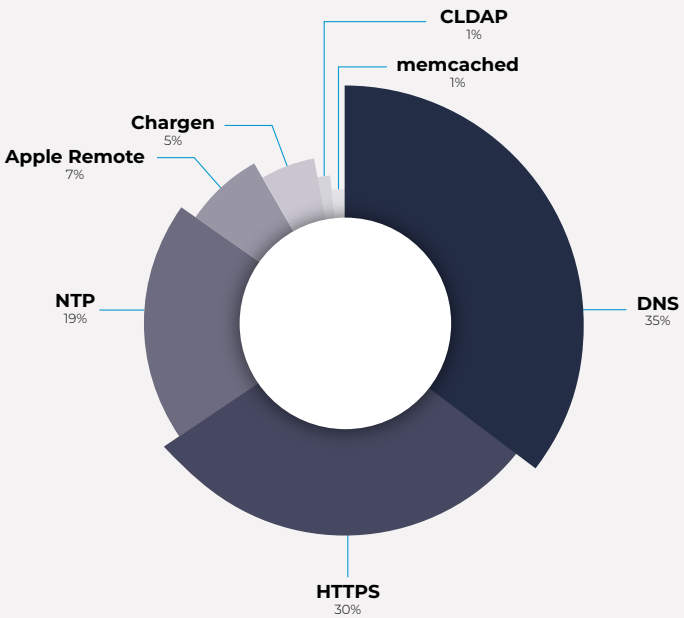


Im ersten Halbjahr 2023 hat der Anteil der Multi-Vektor-Angriffe im Vergleich zum Vorjahr zugenommen. Während in den ersten sechs Monaten 2023 der Anteil von Multi-Vektor-Attacken bei 52 % lag, waren in der ersten Jahreshälfte 2022 nur rund ein Drittel der Attacken (35 %) multidimensionale Angriffe. Statt solch multidimensionaler Angriffe, bei denen es sich um mehrere gleichzeitig laufende Attacken handelt, bevorzugten die Angreifer im Vorjahreszeitraum ressourcenschonendere Attacken.

Nachdem im vergangenen Jahr die bisher größte Multi-Vektor-Attacke im Netzwerk von Link11 (18 Vektoren) beobachtet wurde, betrug die Anzahl gleichzeitig eingesetzter Vektoren im aktuellen Betrachtungszeitraum nur 11. Die Angriffe zeichnen sich jedoch dadurch aus, dass sie komplexer werden. Das bedeutet, dass die Angreifer in kürzester Zeit die Angriffsvektoren rotieren lassen, um größtmöglichen Schaden anzurichten.

Die größte Veränderung, gemessen am Angriffsvolumen, zeigt sich bei HTTPS-Attacken (30 %). Hier lässt sich ein deutlicher Anstieg an Layer-7-Angriffen erkennen. In mehr als einem Drittel (35 %) der Multi-Vektor-Attacken ist DNS als Vektor eingesetzt worden, in rund einem Fünftel (19 %) nutzten die Angreifer NTP.

Angriffsvektoren 1. Halbjahr 2023



Mit jedem neuen Angriffsvektor, der bei einer komplexen Multi-Vektor-Attacke hinzukommt, wird die Identifizierung der einzelnen Vektoren schwieriger. Man könnte sagen, dass im bösartigen Datenverkehr mit jedem Vektor eine Menge zusätzliches „Rauschen“ hinzugefügt wird. Dieses Rauschen erschwert es, die Multi-Vektor-Attacken zu identifizieren. Denn es ist viel einfacher, eine Botschaft zu verstehen, wenn 1.000 Leute dasselbe sagen, als wenn sie 1.000 unterschiedliche Aussagen treffen.

Genauso verhält es sich mit den Vektoren: Fügt man mehr und mehr Vektoren hinzu, wird es schwieriger, jeden einzelnen Angriff aus der Masse heraus zu identifizieren. Dazukommt, dass mehr dieser Angriffe ihr Ziel erreichen, weil sie entweder falsch identifiziert wurden oder die Schutzlösung keine Abwehrmaßnahmen für diesen einen bestimmten Vektor bereithält. Je mehr Angriffe es insgesamt gibt, desto komplizierter ist es, sie abzuwehren. Das bedeutet im Umkehrschluss, dass die Erfolgsaussichten einer Attacke steigen.

„Eine spezialisierte DDoS-Schutzlösung, die eine kontinuierliche Überwachung gewährleistet und Angriffe in Echtzeit erkennen und abwehren kann, schützt vor den Gefahren von Multi-Vektor-Attacken. Damit ist auch das Risiko längerer Ausfallzeiten und potenziellen Folgeschäden reduziert.“

Jag Bains, Vice President Solution Engineering, Link11

Reflection-Amplification-Angriffe

Oldie but Goldie: Memcached und Chargen – populäre Verstärkungsfaktoren

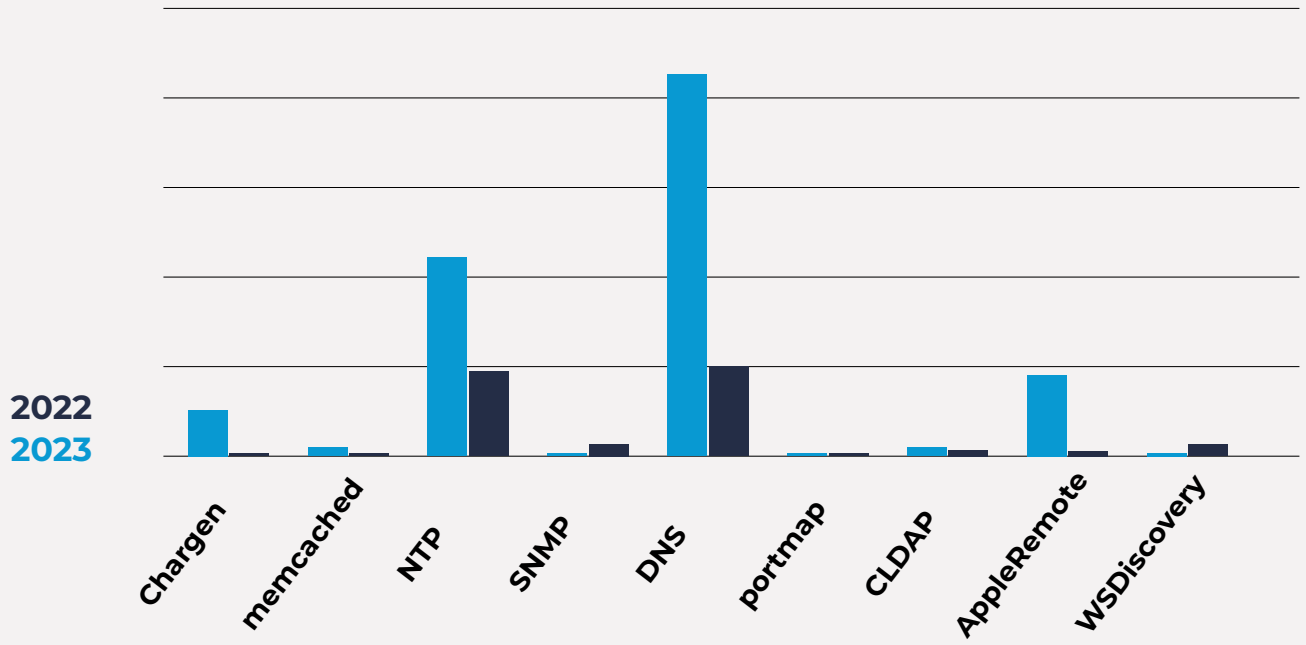
Reflection-Amplification-Angriffe sind eine Klasse von Multi-Vektor-Angriffen, die verschiedene falsch konfigurierte offene Server und Services im Internet auf ähnliche Art ausnutzen. Statt das Ziel direkt anzugreifen, missbrauchen die Angreifer Dienste wie DNS oder NTP. Bei vielen solcher Internetdienste wird die Verifizierung des Absenders nicht unterstützt oder ist nicht erforderlich. Indem der Angreifer den Absender fälscht (auch als Spoofing bekannt), bringt er diese Dienste dazu, unerwünschte Antworten an das tatsächliche Angriffsziel zu senden (Reflection).

Um die Schlagkraft des Angriffes zu erhöhen, werden zunächst kleine Datenmengen an zwischengeschaltete Server gesendet, die als Verstärker dienen. In der Regel wählen Angreifer Dienste aus, deren Antworten um ein Vielfaches größer sind als die ursprüngliche Anfrage. Das steigert die Menge des gesendeten Datenverkehrs enorm. Die missbrauchten Server spiegeln die Anfragen und leiten sie vielfach verstärkt (Amplification) an das eigentliche Angriffsziel weiter.

Von Januar bis Ende Juni 2023 hat das LSOC mehr als ein Dutzend Verstärkertechniken registriert. Viele dieser Angriffstechniken, wie DNS und NTP, zählen bereits seit 2013 zur Standard-Ausrüstung von DDoS-Angreifern. Diese Techniken zeichnen sich durch eine immense Steigerung aus, beispielsweise durch eine 100-fache bei DNS-Attacken und bis zu 200-fache Verstärkung bei NTP-Angriffen.

Obwohl Angreifer neue Schwachstellen wie unzureichend geschützte Internetdienste und offene Dienste entdecken, wurden im Betrachtungszeitraum für die meisten Angriffe bereits bekannte und altbewährte Vektoren eingesetzt. Der Internetdienst, der im ersten Halbjahr 2023 am häufigsten für Angriffe ausgenutzt und als Verstärker missbraucht wurde, war DNS. Gefolgt von NTP, Apple Remote, Chargen und Memcached.

Reflection-Amplification-Vektoren I 1. Halbjahr 2023 vs. 1. Halbjahr 2022



Memcached ist nach wie vor der größte Verstärkungsfaktor, der im Betrachtungszeitraum wieder an Popularität gewonnen hat. Mit der Hilfe von Memcached können Angreifer mit einer 15-Byte-Anfrage eine 750 Kilobyte große Antwort erzeugen. Das entspricht einem Verstärkungsfaktor von über 50.000. Memcached ist ein Datenbank-Caching-System, das zum Speichern und schnellen Abrufen beliebig kleiner Datenmengen verwendet wird.

Die Angreifer erstellen zunächst eine Datennutzlast in einem verfügbaren Memcached-Server. Dann schicken sie eine HTTP-GET-Anfrage an den Memcached-Server. Dabei geben sie sich als das Opfer aus (Spoofing). Im nächsten Schritt antwortet der Server auf die Anfrage und sendet eine große Datenmenge an die IP-Adresse des tatsächlichen Opfers. Mit der meist sehr großen Datenmenge ist der Server im Rechenzentrum des betroffenen Unternehmens überlastet und nicht mehr für legitime Nutzer erreichbar.

Die Angreifer erstellen zunächst eine Datennutzlast in einem verfügbaren Memcached-Server. Dann schicken sie eine HTTP-GET-Anfrage an den Memcached-Server. Dabei geben sie sich als das Opfer aus (Spoofing). Im nächsten Schritt antwortet der Server auf die Anfrage und sendet eine große Datenmenge an die IP-Adresse des tatsächlichen Opfers. Mit der meist sehr großen Datenmenge ist der Server im Rechenzentrum des betroffenen Unternehmens überlastet und nicht mehr für legitime Nutzer erreichbar.

Neben Memcached hat ein weiterer sehr alter Reflection-Amplification-Angriff an Popularität gewonnen: das Chargen-Protokoll, auch bekannt als Character Generator Protocol. Der seit 1983 definierte Netzdienst wird seit mehreren Jahren für verstärkte DDoS-Angriffe ausgenutzt, da er noch immer standardmäßig auf internetfähigen Druckern oder Kopieren verwendet wird. Das Chargen-Protokoll kann sowohl über das TCP- als auch das UDP-Protokoll angesprochen werden.

Die häufigste Form dieser Angriffe nutzt *Chargen* als Verstärker für UDP-basierte Angriffe mit IP-Spoofing. Der Vorgang ist simpel: Der Angreifer mobilisiert sein Botnetz, um Zehntausende Chargen-Anfragen an öffentlich zugängliche Systeme zu senden, die diesen Dienst anbieten. Bei den Anfragen wird das UDP-Protokoll genutzt und die Bots verwenden die IP-Adresse des tatsächlichen Ziels als Absender-IP. Dadurch werden die Antworten des Chargen-Dienstes nicht an den Angreifer, sondern direkt an das Angriffsziel geschickt. Das Ziel versucht, die Abfragen zu verarbeiten. Jedoch überwältigt die enorme Datenmenge das Ziel und die Server werden in die Knie gezwungen.

Gut funktionierende DDoS-Schutzlösungen sind für Unternehmen unverzichtbar, da die Angriffe immer raffinierter werden. Um den neuesten Bedrohungen gewachsen zu sein, müssen Unternehmen sicherstellen, dass ihre Schutzmaßnahmen regelmäßig aktualisiert werden. Ein effektiver Schutz ermöglicht es, schnell auf Angriffe zu reagieren, sie zu erkennen und innerhalb kürzester Zeit zu entschärfen.

”

„Angreifer nutzen sowohl altbekannte als auch neue Schwachstellen für DDoS-Angriffe. Obwohl das Missbrauchspotenzial schon so lange bekannt ist, werden die Sicherheitslücken häufig nur unzureichend gepatcht. Inzwischen ist kein UDP-Service mehr vor Missbrauch sicher, da Angreifer permanent nach neuen Ports und Protokollen suchen, um IT-Infrastrukturen zu überlasten.“

Jag Bains, Vice President Solution Engineering, Link11

Ausblick

Künstliche Intelligenz - Chance für Cybersecurity, Potenzial für Cybercrime

Ende März 2023 hat Europol, die Strafverfolgungsbehörde der Europäischen Union, ihren jüngsten Bericht über ChatGPT mit dem Titel „The Impact of Large Language Models on Law Enforcement“ veröffentlicht.[35] Darin warnt Europol vor dem möglichen kriminellen Missbrauch von Textrobotern wie ChatGPT, die auf künstlicher Intelligenz (KI) basieren.

ChatGPT ist ein von OpenAI entwickelter Chatbot, der auf der Generative Pretrained Transformer-Serie oder kurz GPT großer Sprachmodelle basiert. *Das „Large Language Model“ ChatGPT* kann Texte schreiben, Musik erzeugen und Code generieren. Seit dem Start im November 2022 hat die Technologie aufgrund ihrer beeindruckenden Fähigkeiten viel Aufmerksamkeit erregt.

Wie auch Europol betont, kann diese Technologie daher für Betrug, Falschinformation und Cybercrime eingesetzt werden. Menschen können durch authentisch klingende Texte getäuscht werden – die kriminelle Variante WormGPT ist bereits in der Lage, täuschend echte Phishing-Mails zu generieren.[36] Auch das FBI warnt vor dieser Entwicklung.[37]

Auch wenn Angreifer zunehmend künstliche Intelligenz nutzen, um ihre Methoden und Angriffstypen zu verbessern, hat ChatGPT ein neues Level freigeschaltet. Denn während generative KI vielen von uns das Leben erheblich erleichtern kann, macht sie leider auch die Arbeit von Cyberkriminellen leichter. Mit der Hilfe von ChatGPT können selbst unerfahrene Angreifer anspruchsvollere Angriffe wie Phishing-Kampagnen starten oder Malware schreiben und diese in einer Excel-Tabelle verstecken.

Für das World Economic Forum[38] gehören die folgenden Angriffstechniken zu den größten Risiken:

- bessere Malware entwickeln,
- personalisierte Phishing-Mails,
- Deepfakes generieren,
- Passwörter und Captchas umgehen,
- täuschen KI-basierter Sicherheitssysteme.

Der Wettlauf zwischen Angreifern und Verteidigern verschärft sich. Künstliche Intelligenz wird zwar böswillige Hacker noch nicht komplett ersetzen, gleichzeitig beschleunigt sie ihre Arbeit.[39] Vor allem bei der Mustererkennung und der Korrelation großer Datenmengen ist KI sehr gut.

Gleichzeitig können Verteidiger jedoch auch KI nutzen, um Bedrohungen schneller zu identifizieren und Organisationen besser und effektiver als je zuvor zu schützen. Intelligente und robuste DDoS-Schutzlösungen wie die KI-gestützte, cloudbasierte Lösung von Link11 können dazu beitragen, dass Verteidiger in diesem Rennen die Oberhand behalten.

Der *Link11-DDoS-Schutz* hat dank des eingesetzten Machine Learnings einen nachweislichen Vorteil gegenüber modernen Angriffen. Das Link11-System ist in der Lage, jedes Jahr aus Tausenden Angriffen zu lernen. Mit der wachsenden Anzahl offensiver KI-basierter Angriffssysteme werden sich diese Trainingsdaten entsprechend vervielfachen. Das macht die Schutzlösung nicht nur intelligenter und schneller, sondern auch nachweislich sicherer.

Neue Richtlinien verschärfen Cybersicherheitsstandards

Die Europäische Union hat am 16. Januar 2023 die neue europäische Richtlinie zur Netz- und Informationssicherheit (NIS2)[40] veröffentlicht.[41] Die Richtlinie hat eine Umsetzungsfrist für die Mitgliedstaaten bis zum 17. Oktober 2024 und zielt darauf ab, die Cybersicherheit zu verbessern und zu erweitern.

Damit verschärfen die europäischen Gesetzgeber die Cybersicherheitsstandards und fordern die vollständige Offenlegung von Sicherheitsvorfällen unter Androhung harter Strafen. Neben der neuen EU-Richtlinie NIS2 werden bestehende IT-Sicherheitsgesetze in Deutschland zusätzlich durch das KRITIS-DachG[42] erweitert und an die gestiegene Bedrohungslage angepasst.

Wesentliche Punkte der neuen EU-Richtlinie NIS2 und des KRITIS-DachG für Deutschlands Cybersicherheit sind:

1. Erweiterter Anwendungsbereich: Die neuen Regelungen erfassen eine Vielzahl von Unternehmen, insbesondere kritische Infrastrukturen. Die NIS2-Richtlinie umfasst „wesentliche“ und „wichtige“ Einrichtungen, während das KRITIS-DachG die „kritischen Infrastrukturen“ sowie „kritische Anlagen“ einschließt.

2. Anforderungen an die Unternehmen: Die Betreiber von kritischen Infrastrukturen müssen umfassende Maßnahmen zur Sicherheit und Resilienz umsetzen, die sich grob in Vorgaben zum Risikomanagement, Registrierungspflichten, Meldepflichten und Nachweisen getroffener Maßnahmen unterteilen lassen. Die Unternehmen müssen den „Stand der Technik“ beachten und die Geeignetheit und Verhältnismäßigkeit der Maßnahmen prüfen.

3. Management-Verantwortlichkeit: Die Geschäftsleitung trägt eine erweiterte Verantwortung für die Sicherheit und Resilienz des Unternehmens. Sie muss die getroffenen Risikomanagementmaßnahmen zur IT-Sicherheit billigen und überwachen. Die persönliche Haftung der Geschäftsleitung für Schäden durch mangelhafte Risikomanagementvorgaben ist vorgesehen und die Geschäftsleitung muss sich ausreichende Fachkenntnisse zur Bewertung der Maßnahmen aneignen.

4. Bußgelder und Sanktionen: Bei Verstößen gegen die neuen Gesetze drohen hohe Bußgelder bis zu 10 Millionen Euro oder zwei Prozent des weltweiten Vorjahresumsatzes eines Unternehmens. Die Sanktionen sollen hinreichend wirksam und abschreckend sein.

Die Cybersicherheit in Deutschland steht vor einem bedeutenden Wandel, der eine verstärkte Auseinandersetzung mit IT-Sicherheit und Resilienz in Unternehmen erfordert und die Verantwortlichkeit des Managements in den Fokus rückt. Um die zunehmenden Cyberbedrohungen angemessen bewältigen zu können, müssen die neuen Gesetze professionell umgesetzt werden.

Nachweise

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

[2] https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/

[3] What The Hell Is Darknet Parliament? – LiveDarknet

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

[5] https://cybernews.com/news/european-investment-bank-cyberattack-russia/

[6] https://cybernews.com/security/microsoft-outlook-outage-anonymous-sudan/

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

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

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

[10] https://cybernews.com/cyber-war/russian-killnet-targets-us-hospitals/

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

[12] https://www.scmagazine.com/news/threats/danish-hospitals-latest-target-of-ddos-attacks-on-nato-backed-countries

[13] https://www.bleepingcomputer.com/news/security/tor-and-i2p-networks-hit-by-wave-of-ongoing-ddos-attacks/

[14] https://www.tagesschau.de/inland/regional/nordrheinwestfalen/wdr-story-54483.html

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

[16] https://cybernews.com/news/kremlin-hackers-strike-french-parliament/

[17] https://www.tagesschau.de/inland/cyberattacken-103.html

[18] https://www.cbc.ca/news/canada/montreal/hydro-quebec-website-cyberattack-1.6808947

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

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

[21] https://cybernews.com/cyber-war/russian-hackers-hit-polish-news-sites-ddos-attack/

[22] https://www.euractiv.com/section/politics/news/heightened-cyber-attacks-threat-before-council-of-europe-summit-in-reykjavik/

[23] https://cybernews.com/security/microsoft-outlook-outage-anonymous-sudan/

[24] https://www.swissinfo.ch/eng/politics/swiss-government-and-federal-railways-hit-by-cyberattacks/48583086

[25] https://cybernews.com/news/european-investment-bank-cyberattack-russia/

[26] https://www.emcrc.co.uk/post/killnet-declare-war-on-the-uk-and-nine-other-nations

[27] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

[28] https://www.sueddeutsche.de/wirtschaft/russland-cyberangriffe-bsi-claudia-plattner-1.6000089?reduced=true

[29] https://www.darkreading.com/risk/killnet-threatens-imminent-swift-world-banking-attacks

[30] https://files.truesec.com/hubfs/Reports/Anonymous%20Sudan%20-%20Publish%201.2%20-%20a%20Truesec%20Report.pdf

[31] https://www.bloomberg.com/news/articles/2023-06-28/anonymous-sudan-does-group-behind-microsoft-cyberattack-have-ties-to-russia

[32] https://cybernews.com/editorial/anonymous-sudan-explained/

[33] https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/

[34] https://www.csoonline.com/de/a/neue-malware-baut-bot-netze-auf,3674449

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

[36] https://www.golem.de/news/chatbot-fuer-cyberkriminelle-wormgpt-generiert-aeusserst-ueberzeugende-phishing-mails-2307-175894.html

[37] https://www.fbi.gov/news/speeches/director-wray-s-remarks-to-the-atlanta-commerce-and-press-clubs

[38] https://www.weforum.org/agenda/2023/01/davos23-generativeai-technology-artificial-intelligence/

[39] https://www.bugcrowd.com/blog/inside-the-mind-of-a-hacker-2023-edition/

[40] https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

[41] https://www.consilium.europa.eu/de/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

[42] https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2022/12/kritis-dachgesetz.html

Kontakt

Link11 GmbH
Lindleystr. 12
60314 Frankfurt