LINK11

DDOS-REPORT

2022

www.link11.com

Inhalt

Aktuelle Bedrohungslage und Zusammenfassung

Adaptiv, komplex und gefährlich – DDoS-Angriffe und ihre Metamorphose

Mehr als zwei Jahre lang hat die Corona-Pandemie das gesellschaftliche Leben und die Wirtschaft beeinflusst. Für den Bitkom „Digital Office Index 2022“ gab jedes zweite der befragten Unternehmen an, dass Corona die digitale Transformation beschleunigt hat.[1] Das gilt besonders für hybride Arbeitsmodelle, Migration in die Cloud und Verbesserungen unternehmenseigener IT-Services sowie Web-Services, die den beruflichen Alltag sicherstellen.

Obwohl Cybervorfälle bereits durch die Corona-Pandemie und dem damit verbundenen Digitalisierungsschub deutlich zugenommen haben, hat sich die Lage mit dem Beginn des Krieges in der Ukraine am 24. Februar 2022 weiter zugespitzt. Das BSI konstatiert im aktuellen Lagebericht, die Bedrohungslage sei „so hoch wie nie“[2].

Die pro-russische Hackergruppe „Killnet“ hat mehreren Ländern, darunter auch Deutschland, den Cyberkrieg erklärt.[3] In Deutschland, Italien, Litauen, Norwegen und Polen waren die Folgen dieser Erklärung bereits zu spüren.[4] Es verging kaum ein Monat, in dem es keinen Cyberangriff auf NATO-Staaten, deren öffentlichen Institutionen, Banken oder kritische Infrastrukturen gab.

Zwar setzen Cyber-Akteure auch in Friedenszeiten ausgeklügelte Schadsoftware oder komplexe DDoS-Angriffe ein, doch durch den Einsatz als Waffe im Cyberkrieg können die Folgen weitaus verheerender sein. Dabei geht es den Angreifern vor allem darum, die Moral der Kämpfenden und der Bevölkerung zu schwächen und größtmöglichen Schaden anzurichten, wie auch Microsoft im Report „Defending Ukraine: Early Lessons from the Cyber War“[5] festgestellt hat.

Aktuell erleben wir eine sehr dynamische Situation: Während das Link11 Security Operations Center (LSOC) 2022 noch einen Rückgang beobachtet hat, vergeht seit der Bekanntgabe der Bundesregierung zur Unterstützung der Ukraine mit Kampfpanzern im Januar 2023 kaum ein Tag, an dem in den Medien nicht von DDoS-Angriffen insbesondere auf Betreiber kritischer Infrastrukturen (KRITIS) berichtet wird. Auch das niederländische National Scrubbing Center (NaWas) hat seit Ende 2021 weniger DDoS-Angriffe registriert.[6]

Nach wie vor ist der langfristige Trend zunehmender Cyberangriffe ungebrochen. Den Experten des Weltwirtschaftsforums zufolge zieht ein regelrechter „Cyber-Sturm“[7] auf. Aus dem aktuellen „Global Cybersecurity Outlook“ geht zudem hervor, dass 91 % der befragten Führungskräfte von weitreichenden und katastrophalen Cybervorfällen in den kommenden Jahren ausgehen.

Für den ersten temporären Rückgang der Angriffe im Vergleich zum DDoS-Rekordjahr 2021 um mehr als drei Viertel (79 %) gibt es verschiedene Gründe. Die massive Zunahme politisch motivierter DDoS-Attacken – auch aufgrund weiterer geopolitischer Spannungen wie zwischen China und Taiwan sowie zwischen den USA, Israel und dem Iran – führte zu einer Verlagerung der Angriffe. Zudem suchten sich die Angreifer leichte Ziele in Form von ungesicherten oder nicht wirksam geschützten Systemen.

Darüber hinaus führte im April 2022 eine erfolgreiche Zusammenarbeit zwischen dem BKA und dem US-Justizministerium zur Schließung des größten illegalen Online-Marktplatzes „Hydra“[8] im Darknet. Im Dezember 2022 schlugen das FBI und Europol erneut gegen DDoS-Kriminalität zu, indem sie 48 illegale DDoS-for-hire-Dienste, sogenannte „Booter-Services“, geschlossen haben.[9] Solche Aktionen sind kurze Verschnaufpausen, bis sich die Hacker mit neuen Plattformen wieder einen Namen machen konnten und verstärkt aktiv sind.

In den Jahren 2020 und 2021 waren mehrere Wellen von DDoS-Erpressungen (RDDoS – Ransom Distributed Denial of Serivce) durch Armada Collective, Fancy Bear, Lazarus-Group oder Fancy Lazarus eine der großen Triebkräfte. Seit diesen Höhepunkten hat es jedoch weniger RDDoS-Attacken gegeben, da die üblichen Akteure auf dem Cybercrime-Spielfeld ihre Kapazitäten auf andere Ziele oder politisch motivierte Angriffe konzentrierten.

Es sind zwar weniger Angriffe, gleichzeitig werden sie gefährlicher. Das LSOC hat beobachtet, dass sich diese Attacken und die angewandten Methoden ständig verändern. Statt willkürlich in der Hoffnung auf Erfolg die Unternehmen zu attackieren, kommen nun sehr gezielt fortgeschrittene und ausgeklügelte DDoS-Attacken zum Einsatz.

Die im Betrachtungszeitraum 2022 verzeichneten Angriffe waren kürzer, intensiver und anspruchsvoller. Die Analyse der im Link11-Netzwerk registrierten Attacken zeigt, dass die kritische Last bei den DDoS-Angriffen im Jahr 2022 im Durchschnitt bereits 55 Sekunden nach Beginn der Attacke erreicht wurde. Im Vergleich dazu benötigten Angriffe im Jahr 2021 durchschnittlich 184 Sekunden, um ihren Höhepunkt zu erreichen. Diese „Turboangriffe“ können das Netzwerk bereits vor der Wirksamkeit der Verteidigungsmaßnahmen lahmlegen, sofern ein im Hinblick auf Präzision und Geschwindigkeit der Mitigation hochperformantes Abwehrsystem wie das von Link11 fehlt.

Der Trend zu volumenstarken Angriffen, der sich bereits Ende 2021 abzeichnete, hat sich zwar im ersten Halbjahr 2022 verstetigt. Im direkten Vergleich mit dem Vorjahr waren die Bandbreiten-Peaks im Durchschnitt jedoch größer. Während die vom LSOC gemessenen Bandbreiten im Jahr 2021 jeden Monat 100 Gbit/s überstiegen, ist das Jahr 2022 von deutlichen Schwankungen geprägt. Im Oktober und November 2022 liegen die Bandbreiten-Spitzenwerte sogar deutlich unter 100 Gbit/s.

Im ersten Halbjahr 2022 hat der Anteil der Multi-Vektor-Angriffe im Vergleich zum Vorjahreszeitraum abgenommen. Während 2021 der Anteil von Multi-Vektor-Attacken bei 71 % lag, waren in den ersten sechs Monaten nur rund ein Drittel der Attacken (35 %) multidimensionale Angriffe. Insgesamt ist der Anteil der Multi-Vektor-Attacken von Juli bis Dezember 2022 auf 45 % gestiegen, wobei der deutlichste Anstieg im 4. Quartal zu erkennen ist.

Zusammenfassend lässt sich feststellen: DDoS-Angriffe sind enorm wandlungsfähig. Ihre DNA verändert sich kontinuierlich und sie werden permanent an die Bedingungen in der Cyberlandschaft angepasst. Das macht sie zu einer unberechenbaren Gefahr für Organisationen aller Art und Größe. Das von „Hydra“ und anderen hinterlassene Vakuum wird von noch unbekannten Parteien gefüllt, was die Ungewissheit zukünftig vergrößert.

DDoS in den Nachrichten

Januar 2022

Kein Internet in Andorra: Angriff auf Minecraft-Spieler legt Internet lahm

Durch DDoS-Angriffe auf den Internet Service Provider (ISP) in Andorra während eines Twitch-Gaming-Turniers wurden mehrere Minecraft-Spieler aus einem Turnier geworfen und das Internet im ganzen Land lahmgelegt.[10]

Februar 2022

DDoS-Angriffswelle auf die Ukraine

Vor dem russischen Einmarsch in die Ukraine kam es zu mehreren DDoS-Attacken auf staatliche Institutionen wie das Verteidigungsministerium und staatliche Banken.[11]

März 2022

Angriff auf nationalen ukrainischen Internet-Provider

Das Internet in der Ukraine fällt nach einem Angriff auf Ukrtelecom, dem nationalen Internetprovider, 15 Stunden lang aus.[12]

April 2022

Russische Hackergruppe „Killnet“ greift rumänische Regierungsseiten an

Mehrere öffentliche, von staatlichen Stellen verwaltete Websites in Rumänien waren von einer Reihe von DDoS-Angriffen betroffen. Dazu gehörte u. a. die offizielle Website der rumänischen Regierung und die des rumänischen Verteidigungsministeriums.[13]

April 2022

Online-Portal der hessischen Polizei nach DDoS-Angriffen offline

Aufgrund von DDoS-Attacken hat die hessische Polizei ihr Online-Portal vorübergehend aus dem Netz genommen.[14]

Mai 2022

DDoS-Attacken „größeren Ausmaßes“ gegen E-Mail-Dienst Posteo

Der E-Mail-Dienst-Anbieter Posteo hat seit Dienstag mit Distributed-Denial-of-Service-Attacken (DDoS) „größeren Ausmaßes“ zu kämpfen. Im Gegensatz zu früheren Angriffen habe es bisher keine Geldforderungen im Kontext der Angriffe gegeben.[15]

Mai 2022

Angriff auf Eurovision Songcontest und die darauffolgenden Attacken gegen italienische Behörden

Nach der pro-russischen Attacke auf den Eurovision Songcontest, der erfolgreich von der italienischen Polizei abgewehrt wurde, gab es Angriffe auf italienische Behörden.[16]

Mai 2022

Hackerangriff auf deutsche Behörden

Mehrere Websites deutscher Behörden und Ministerien waren von DDoS-Attacken betroffen. Dabei handelte es sich wahrscheinlich um einen pro-russischen Hacker-angriff.[17]

Mai 2022

Website des Londoner Hafens unter Beschuss

Der Londoner Hafen wurde ebenfalls von einer DDoS-Attacke getroffen. Dahinter soll eine pro-iranische Hackertruppe stecken.[18]

Juni 2022

Norwegen Ziel eines Cyberangriffes

Eine Reihe von privaten und öffentlichen Einrichtungen in Norwegen waren Opfer eines sogenannten DDoS-Angriffes. Hinter den Angriffen scheint eine kriminelle pro-russische Gruppe zu stecken, so die norwegischen Sicherheitsbehörden.[19]

Juni 2022

DDoS-Angriff auf Kryptowährung-Plattform Tether

Die Anfragen auf die Website der Kryptowährung Tether stiegen durch einen DDoS-Angriff um mehr als 400 % von zweitausend auf acht Millionen alle fünf Minuten.[20]

Juli 2022

Internetprovider offline

Nach einer massiven DDoS-Attacke auf den lokalen Internet- und Telekommunikationsanbieter Helinet war das Internet nur noch im Schneckentempo zu erreichen.[21]

Juli 2022

Störung der Website des US-Kongresses

Pro-russische Hacker bekannten sich zu einem Cyberangriff, der den Zugang zu einer Website des US-Kongresses am Donnerstagabend kurzzeitig unterbrochen hat.[22]

August 2022

DDoS-Attacke auf Energieunternehmen in Oldenburg

Das Oldenburger Energieunternehmens EWE war von einem intensiven DDoS-Angriff betroffen.[23]

August 2022

DDoS-Angriffe auf taiwanesische Websites

Der Besuch der Sprecherin des Repräsentantenhauses, Nancy Pelosi löste eine DDoS-Attacke auf taiwanesische Websites aus.[24]

September 2022

Cyber-Angriff auf Irans Zentralbank

Irans Zentralbank hat einen Cyber-Angriff auf ihre Systeme bestätigt. Die Bank war Ziel einer DDoS-Attacke geworden.[25]

September 2022

Pokerturniere abgesagt

Alle sechs WCOOP Main Events von PokerStars sind aufgrund von DDoS-Attacken ausgefallen und mussten verschoben werden.[26]

Oktober 2022

US-Flughafen-Websites von Cyberangriffen betroffen

Die DDoS-Angriffe einer pro-russischen Hackergruppe betrafen die Flughafen-Websites mehrerer großer US-Städte, darunter Atlanta, Chicago, Los Angeles, New York, Phoenix und St. Louis.[27]

November 2022

Black Tuesday für Trading-Bank Swissquote

Die Bank stand unter einer DDoS-Cyber-Attacke, Kunden hatten keinen Zugriff auf Titel und erhielten keine Kurse.[28]

November 2022

Pro-russische Hacktivisten legen Website des EU-Parlaments mit DDoS-Angriff lahm

Die Website des Europäischen Parlaments wurde nach einem DDoS-Angriff, der von Anonymous Russia (Teil der Killnet-Gruppe) durchgeführt wurde, abgeschaltet.[29]

Dezember 2022

Russlands zweitgrößte Bank VTB attackiert

Die staatliche Bank VTB wurde Opfer eines Cyberangriffs. Die DDoS-Attacken konnte die Bank abwehren.[30]

Dezember 2022

Österreichische Bundesbahn Ziel einer DDoS-Attacke

Die Website der Österreichischen Bundesbahn (ÖBB) und der Ticketkauf sind aufgrund eines DDoS-Angriffes ausgefallen.[31]

Entwicklung der Gesamtzahlen im Link11-Netzwerk

Anzahl DDoS-Angriffe reduziert

DDoS-Attacken haben im Jahr 2022 eine Verschnaufpause erfahren: Nach dem Allzeithoch im Jahr 2021, verzeichnete das LSOC erstmals einen Rückgang der Angriffe im Netzwerk. Im Jahr 2022 sank die Zahl der Attacken um 79 % im Vergleich zum Vorjahr. Die Gründe hierfür sind vielfältig.

Während der Corona-Pandemie stieg die Anzahl der DDoS-Angriffe weltweit an, da Cyberkriminelle die digitale Verwundbarkeit der Unternehmen und der remote arbeitenden Bevölkerung ausnutzen wollten. Das betraf insbesondere wichtige Web-Services wie Impfplattformen, Lernportale und IT-Systeme für das Homeoffice. Neben der Zunahme von Angriffen auf die Infrastrukturen, die das Leben und Arbeiten während der Corona-Pandemie sicherstellten, erstreckten sich die DDoS-Attacken auch auf Hosting-Provider und Internet-Service-Provider.

Seit Kriegsbeginn in der Ukraine im Februar 2022 haben die politisch motivierten DDoS-Angriffe durch den dazugehörigen Cyberkrieg deutlich zugenommen. Die pro-russische Hackergruppe Killnet hat inmitten des anhaltenden Krieges in der Ukraine mehreren Ländern, darunter auch Deutschland, den Cyberkrieg erklärt. Die Folgen dieser Erklärung waren bereits in Italien, Litauen, Norwegen und Polen zu spüren. Es verging kaum ein Monat, in dem es keinen Cyberangriff auf NATO-Staaten, deren öffentlichen Institutionen, Banken oder kritischen Infrastrukturen gab.

Auch wenn die Anzahl der Attacken im Vergleich zum Vorjahreszeitraum zurückgegangen ist, zeigt sich die enorme Wandlungsfähigkeit der DDoS-Attacken. Ihre DNA verändert sich permanent. Umso wichtiger ist es, sich mit einer KI-basierten und automatisierten DDoS-Schutzlösung auf dem neusten Stand auf alle potenziellen Angriffsmodalitäten vorzubereiten.

Killnet ist ein von Russland unterstütztes Cybercrime-Syndikat, das erstmals im Januar 2022 in Erscheinung trat, als es in illegalen Foren DDoS-Dienste anbot. Während der russischen Invasion in der Ukraine bekannte sich die Gruppe zur russischen Regierung und erklärte, dass sie jeden, der sich dem Regime widersetze, feindselig behandle. Seitdem hat Killnet gezielte Angriffe auf Websites in Ländern gestartet, die Russland ablehnend gegenüberstehen, darunter verschiedene NATO-Mitgliedstaaten.

Die Gruppe gilt als eine der aktivsten Hacktivisten-Organisationen, die primär darauf abzielt, Aufmerksamkeit zu erregen, anstatt ernsthaften Schaden anzurichten oder wesentliche finanzielle Vorteile zu erzielen. Killnets neuer Kommandant, Blackside, ist Berichten zufolge ein Experte für Phishing, Ransomware und Krypto-Diebstähle, was darauf hindeutet, dass die Gruppe ihre operativen Fähigkeiten erweitern und verbessern möchte.

Zu den Taktiken von Killnet zählen DDoS-Angriffe und Desinformationskampagnen, mit denen sie die Öffentlichkeit verunsichern. Die Gruppe hat Angriffe auf kritische Infrastrukturen, Flughafen-Websites, Regierungsdienste und Medienunternehmen in NATO-Staaten sowie auf ukrainische Unterstützer in Osteuropa, den nordischen und baltischen Ländern durchgeführt. In der Regel werden bei den Angriffen von Killnet keine Lösegeldforderungen gestellt, und die Kampagnen der Gruppe sowie potenzielle Angriffsziele werden über ihre mehr als 90.000 Telegram-Abonnenten verbreitet.

Killnet verfügt über eine strukturierte Organisationshierarchie und soll mit anderen pro-russischen Hacktivistengruppen, darunter XakNet Team oder Anonymous Sudan, zusammengearbeitet haben. Die lettische Regierung stufte Killnet als terroristische Organisation ein, nachdem die Gruppe für einen Cyberangriff verantwortlich gemacht wurde, der die parlamentarischen Webdienste des Landes vorübergehend lahmlegte. Killnet hatte auch schon öffentliche Auseinandersetzungen mit der Hacktivistengruppe Anonymous.[32]

2022 hat gezeigt, wie dynamisch und unvorhersehbar die Angriffslandschaft ist. Es dominierten politisch motivierte DDoS-Angriffe als Bestandteil im Cyberkrieg. Auch wenn es nach einer Verschnaufpause aussieht, ist die Gefahr nicht gebannt – die Metamorphose der DDoS-Angriffe ist in vollem Gange. Sie werden immer vielfältiger, komplexer und ausgefeilter.

Jens-Philipp Jung, Geschäftsführer, Link11

Die massive Zunahme der politisch motivierten DDoS-Attacken führte dazu, dass die üblichen Akteure auf dem Cybercrime-Spielfeld ihre Kapazitäten auf andere Ziele konzentrierten. Neben dem Ukraine-Krieg sind andere geopolitische Spannungen wie zwischen China und Taiwan sowie zwischen den USA, Israel und dem Iran zu nennen.

Auch im Netzwerk von Link11 bewirkte dies eine Fluktuation im Ursprung der Angriffe. Relativ betrachtet haben sich die Angriffszahlen aus Russland knapp verdoppelt. Auch aus der Ukraine und Taiwan kommen deutlich mehr Angriffe, während es weniger DDoS-Attacken aus den USA und China gab. Zudem suchten sich die Angreifer leichte Ziele, in Form von ungesicherten oder nicht wirksam geschützten Systemen.

Im April 2022 erlebte die Welt einen beispiellosen Schlag gegen das Verbrechen im Darknet: Der größte illegale Online-Marktplatz wurde geschlossen. Deutsche und US-Behörden arbeiteten Hand in Hand, um die Server des russischen „Hydra-Marktes“ zu sichern und 25 Millionen Dollar in Kryptowährung zu beschlagnahmen. Eine erfolgreiche Zusammenarbeit zwischen dem BKA und dem US-Justizministerium führte zu einem bedeutenden Durchbruch im Kampf gegen kriminelle Aktivitäten im Darknet.

Anfang Dezember haben FBI und Europol erneut gegen DDoS-Kriminalität zugeschlagen: 48 Internet-Domains, die illegale DDoS-for-hire-Dienste anboten, wurden beschlagnahmt. Sechs mutmaßliche Täter wurden verhaftet, die für den Betrieb von sogenannten „Booter“-Plattformen verantwortlich waren. Diese Websites ermöglichten es Nutzern, massive DDoS-Angriffe zu starten, die den Zugang zum Internet blockieren können.

Bereits im Jahr 2020 und insbesondere in der ersten Jahreshälfte 2021 waren mehrere Wellen von DDoS-Erpressungen (RDDoS – Ransom Distributed Denial of Serivce) durch Armada Collective, Fancy Bear, Lazarus-Group oder Fancy Lazarus eine große Triebkraft. Nach diesen Höhepunkten der Erpresseraktivitäten gab es bisher deutlich weniger Ransom-DDoS-Attacken.

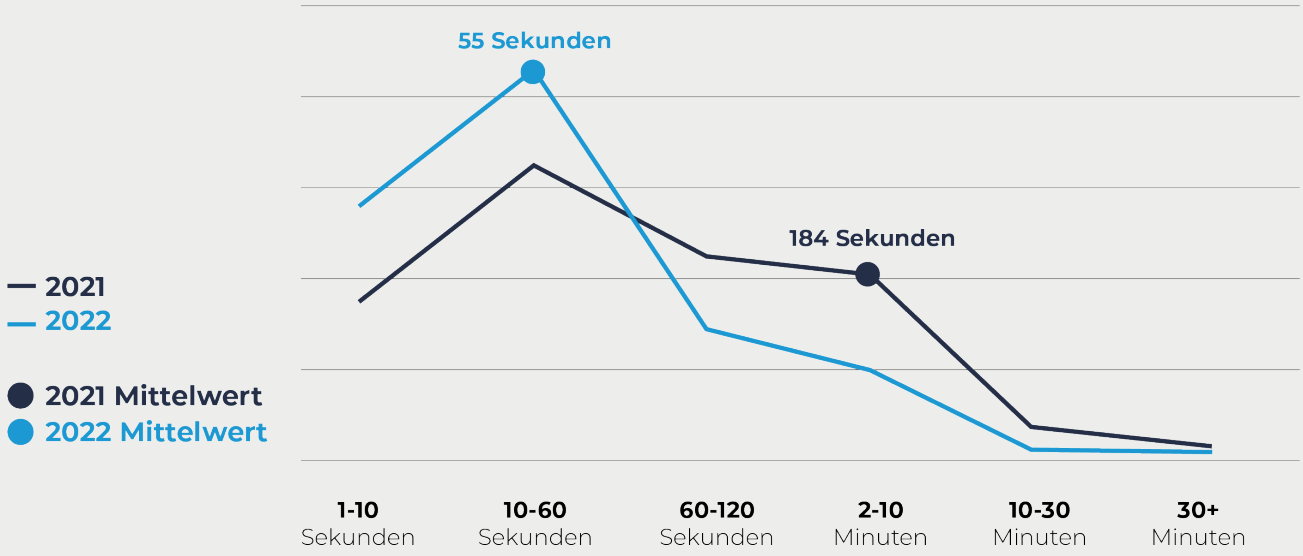
Neue Entwicklungen

Steigende Komplexität – DDoS-Attacken werden herausfordernder

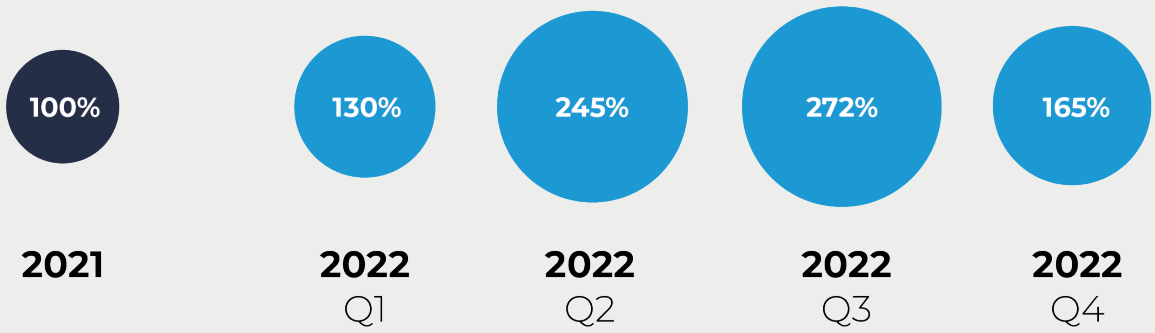
Das LSOC hat erstmalig analysiert, wie lange es dauert, bis DDoS-Attacken ihren Maximalwert erreichen. Hierbei wird im Englischen vom „Onset“, also dem Beginn der Attacke gesprochen. Der Beginn ist die Zeitspanne, die ein Angriff benötigt, um ein kritisches Volumen zu erreichen.

Analysiert wurde, wie viele Sekunden nach der Übertragung der ersten Bytes vergehen müssen, bis der Traffic seinen Maximalwert erreicht. Diese schnell einsetzenden DDoS-Attacken oder „Turboangriffe“ sind in der Regel kürzer. Sie erreichen aber sehr schnell eine kritische Nutzlast, anstatt kontinuierlich anzusteigen. Dadurch können Netzwerksysteme bereits lahmgelegt werden, bevor Abwehrmaßnahmen wirken. In diesem Jahr erreichen DDoS-Angriffe im Durchschnitt bereits nach 55 Sekunden ein kritisches Niveau. Verglichen mit dem Durchschnitt von 184 Sekunden im Jahr 2021 erreichen diese Turbo-Angriffe dreimal schneller ein kritisches Volumen.

Dauer bis zum Höhepunkt einer Attacke | 2021 vs. 2022



Geschwindigkeit bis zum kritischen Angriffsvolumen | 2021 vs. 2022



Besonders im zweiten und dritten Quartal 2022 sind die Angriffe gegenüber dem Vorjahr deutlich rascher eskaliert. Die DDoS-Attacken im zweiten Quartal erreichten ihren Maximalwert um 245 % schneller als im Jahr 2021. Das dritte Quartal war von besonders schnellen „Turboangriffen" geprägt. Das kritische Volumen erzielten die schnelleinsetzenden Attacken um 272 % schneller als im Vorjahr. Damit verkürzte sich für die Ziele eines solchen Angriffes auch die Zeit für die entsprechenden Abwehrmaßnahmen enorm.

Die kurze Dauer eines Angriffes allein ist 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.

Im Link11-Netzwerk wurden im Jahr 2022 Attacken registriert, die doppelt so viel Nutzlast in nur 70 % der Zeit übertragen konnten. In diesem Fall reicht eine TTM von einer Minute nicht aus, um einen kompletten Ausfall zu vermeiden.

> *Zeit ist einer der wichtigsten Faktoren im Angriffsfall, denn jede verstreichende Sekunde kann zu großen Schäden führen – durch manuelle Bewertungen von Vorfällen, unvorhergesehene Routing-Probleme oder überlistete Abwehrmechanismen.*

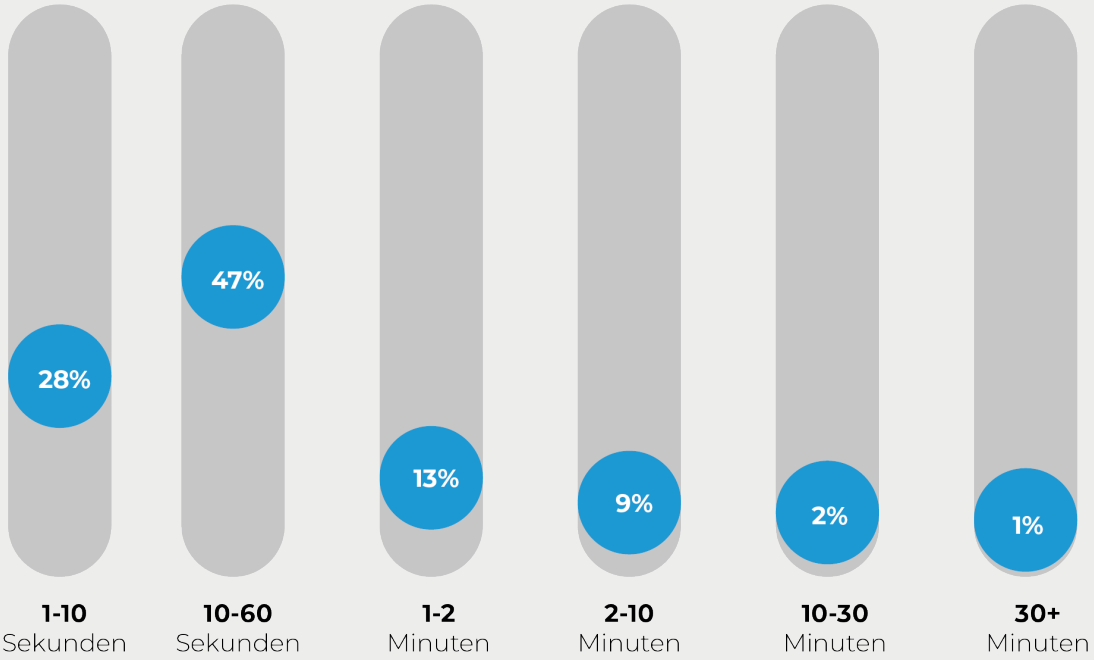
Jag Bains, Vice President Solution Engineering, Link11

Ein Blick auf die Verteilung der Zeit, die während des DDoS-Angriffes bis zum Erreichen des Höhepunktes vergeht, zeigt für 2022 folgende Ergebnisse: In mehr als einem Viertel der Angriffe (28 %) wurde innerhalb der ersten zehn Sekunden die kritische Nutzlast erreicht. Im vergangenen Jahr lag dieser Anteil bei 17 %. Angriffe, die in 10 bis 60 Sekunden ihren Maximalwert erzielten, machten fast die Hälfte aller im Netzwerk registrierten Attacken aus (47 %). Im Vergleich dazu näherten sich ein Drittel der Angriffe (34 %) im Jahr 2021 in der gleichen Zeit ihrem Höhepunkt.

In nur 13 % der Fälle im Jahr 2022 dauerte es zwischen einer und zwei Minuten bei den DDoS-Angriffen, bis der kritische Maximalwert erreicht wurde. Bei mehr als zwei Minuten lag der Anteil bei rund einem Zehntel der vom LSOC verzeichneten DDoS-Angriffe. Im Vergleich zum Vorjahr zeigen sich hier große Unterschiede. Im Jahr 2021 erreichten knapp ein Viertel der Angriffe (23 %) in ein bis zwei Minuten ihren Höhepunkt und in einem Fünftel der Fälle (21 %) dauerte es mehr als zwei Minuten.

Bei einem DDoS-Angriff zählt jede Sekunde. Umso wichtiger ist es, Zeitverluste zu vermeiden, wie beispielsweise bei der manuellen Überprüfung von Vorfällen oder unvorhergesehenen Routing-Problemen. Kommt es dennoch zu solchen Routing-Problemen oder schlüpfen neue Angriffsmethoden durch das Sicherheitsnetz, können diese Verzögerungen in der Abwehr zu großen Schäden führen.

Verteilung der Dauer bis zum Höhepunkt der Attacke



Eine effektive IT-Sicherheitsstrategie setzt daher auf die Analyse des Datenverkehrs in Echtzeit mit smarten, schnellen und sicheren Methoden, 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.

Die Entwicklung der Angriffsdauer

Erst kurz und heftig, dann wieder langanhaltende DDoS-Attacken

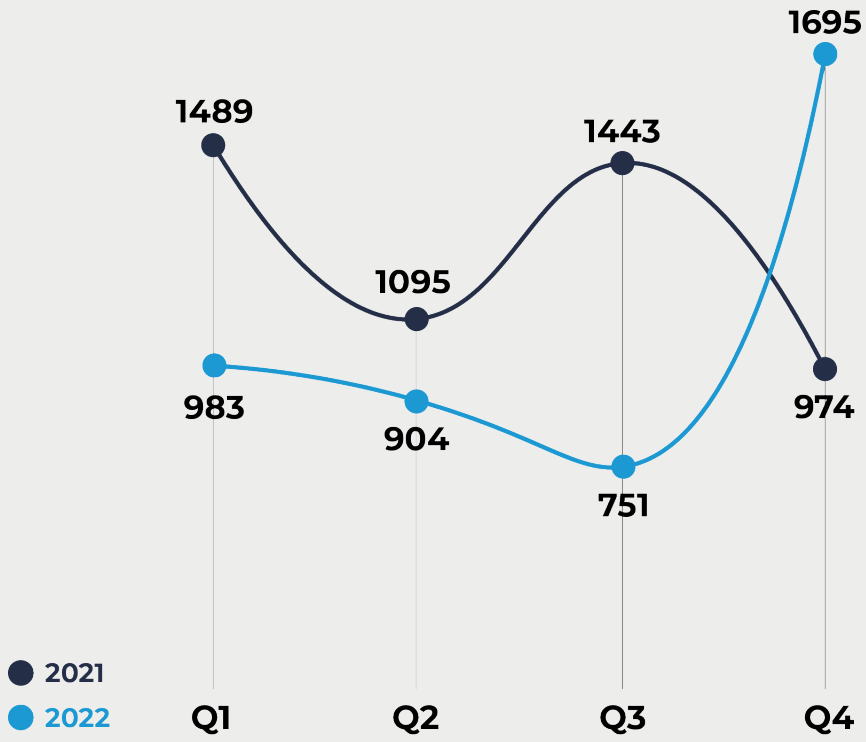
Die Dauer, der im Jahr 2022 im Link11-Netzwerk registrierten DDoS-Angriffe, hat sich im Vergleich zum Vorjahr verkürzt. Zwar gab es fast jeden Monat signifikante Ausreißer, doch die Angriffsdauer ist insgesamt zurückgegangen. Ein Blick auf die Grafik unten zeigt deutlich, wie sich die Dauer der DDoS-Attacken 2022 gegenüber 2021 darstellt.

Insgesamt zeigt sich, dass die jeweils längsten Attacken deutlich voneinander abweichen. Der Trend zu kürzeren DDoS-Angriffen hat sich bereits im vierten Quartal 2021 abgezeichnet. Dieser setzte sich bis ins dritte Quartal 2022 fort. Die Angriffe wiesen im zweiten und dritten Quartal eine besonders geringe Dauer auf. Dies ist charakteristisch für die kurzen, sehr schnell einsetzenden DDoS-Attacken, die verstärkt in diesen beiden Quartalen beobachtet wurden.

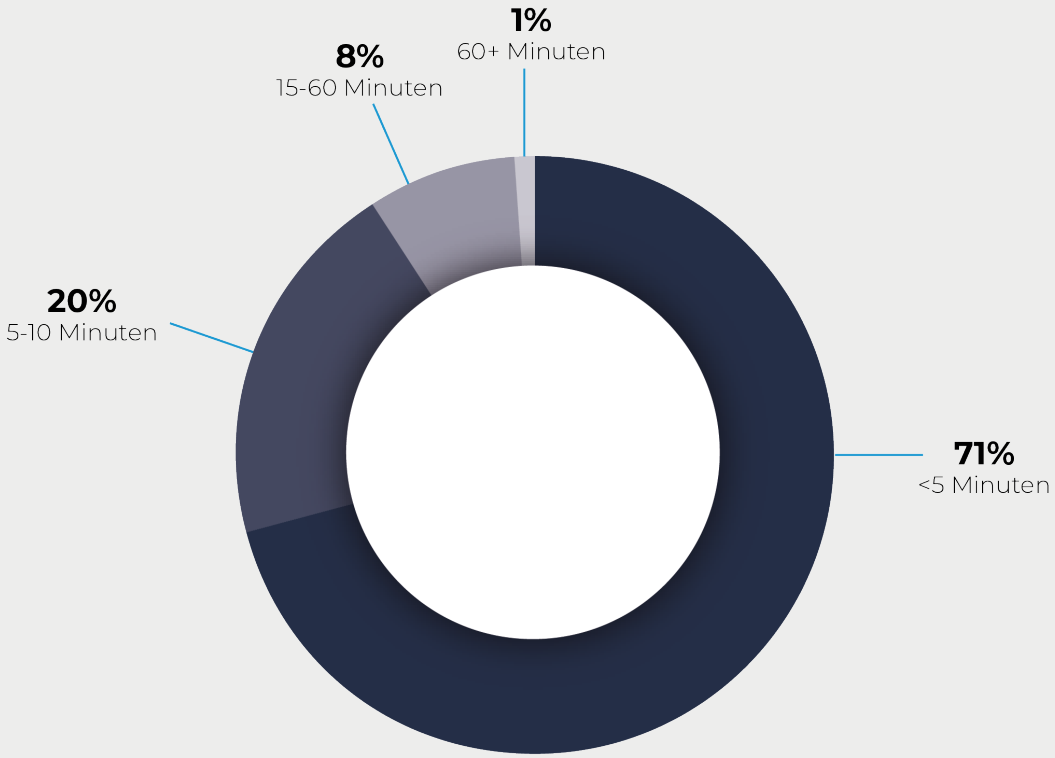
Im vierten Quartal hat die Dauer der Angriffe wieder zugenommen. Die längste Attacke im Jahr 2022 war 1.695 Minuten lang, das entspricht 28 Stunden und 15 Minuten. Der längste DDoS-Angriff 2021 betrug lediglich 1.489 Minuten, also 24 Stunden und 49 Minuten.

Hierin zeigt sich, wie wandlungsfähig die Angriffslandschaft ist. Während in der Jahresmitte schnell einsetzende „Turboangriffe“ überwogen, waren im vierten Quartal 2022 wieder länger anhaltende Multi-Vektor-Attacken zu verzeichnen.

Übersicht Angriffsdauer | 2021 vs. 2022



Übersicht Angriffsdauer 2022



Die weitere Analyse zeigt, dass die Länge der Angriffe zwischen wenigen Minuten und mehreren Stunden schwankte. Der Großteil der Angriffe (71 %) dauerte weniger als 5 Minuten. Ein Fünftel aller registrierten Angriffe (20 %) war zwischen 5 und 15 Minuten lang, weitere 8 % bis zu 60 Minuten. Nur rund 1 % der Angriffe waren länger als 60 Minuten.

Ob es zu kurzen oder langen Angriffen kommt, ist eine Frage der Angriffstechnik. Einerseits scannen Hacker mit Blitzangriffen auf einzelne IP-Adressen die IT-Infrastruktur ihres Zieles nach Schwachstellen ab. Andererseits werden kleine und schnelle DDoS-Attacken in hoher Frequenz als Tarnung für parallele Hacker-Angriffe auf Server und Netzwerke eingesetzt. Doch hinter diesem DDoS-Vorhang können Hacker unbemerkt durch die Hintertür eindringen. Zur Abwehr der DDoS-Attacke werden in kürzester Zeit die vorhandenen IT-Ressourcen mobilisiert, um die Systemausfälle und weitere Schäden zu minimieren.

Kurze Angriffe, die plötzlich abgebrochen werden, sind oft ein Indiz dafür, dass Angreifer ihr Ziel nicht erreichen konnten. Prallen die Angriffe an gut geschützten Infrastrukturen ab, ziehen sich die Angreifer meist zurück, um ihre Ressourcen zu schonen. Doch wenn es ihnen darum geht, die Ziele dauerhaft zu beeinträchtigen und erfolgreich Schäden zu verursachen, greifen sie zu langanhaltenden Attacken.

Entwicklung der Angriffsbandbreiten

DDoS-Angriffe: komplex und kraftvoll

Der bereits im Vorjahreszeitraum erkennbare Trend zu Hochvolumen-Attacken hat sich in den ersten sechs Monaten des Jahres 2022 verstetigt. Noch im ersten Halbjahr lag im Jahresvergleich der Bandbreiten-Peak über den Werten aus 2021. Während im Jahr 2021 die vom LSOC gemessenen Bandbreiten jeden Monat die Marke von 100 Gbit/s überschritten, zeigt die untenstehende Grafik im weiteren Verlauf deutliche Schwankungen für das Jahr 2022. Im Oktober und November 2022 lagen die Bandbreiten-Peaks sogar deutlich unter 100 Gbit/s.

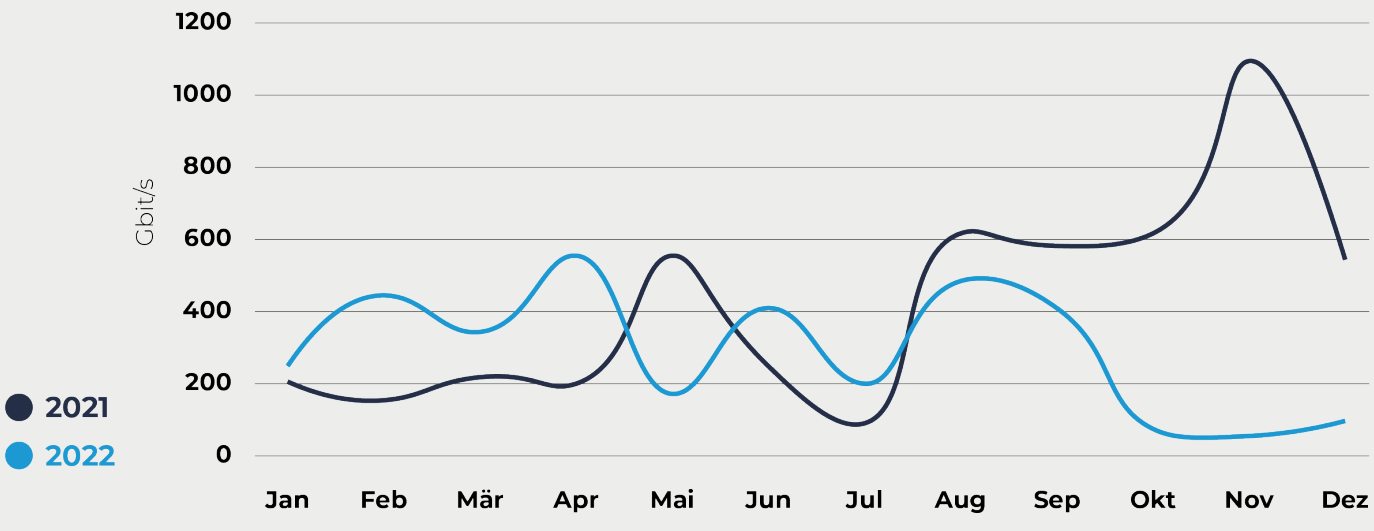
Die größte Attacke im Jahr 2022 wurde bei 574 Gbit/s gestoppt, was im Vergleich zu 2021 niedrig ist. Zwischen August 2021 und Dezember 2021 schwankten die Bandbreiten der Hochvolumen-Attacken zwischen 546 Gbit/s und dem höchsten gemessenen Einzelausschlag von 1,1 Tbit/s. Im vierten Quartal 2022 wurde der größte DDoS-Angriff bei nur 110 Gbit/s gestoppt.

Die durchschnittliche Gesamtbandbreite ist hingegen von 1,4 Gbit/s im Jahr 2021 auf 2,6 Gbit/s gestiegen. Grund hierfür ist weniger „Carpet Bombing“ bei den im Link11-Netzwerk registrierten Attacken. Diese technisch komplexen DDoS-Angriffe sind schwer zu erkennen, da sie einen sehr geringen Datenverkehr pro IP-Adresse aufweisen. 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 von Adressen, was für unzureichend geschützte Hosting- und Cloud-Anbieter fast unmöglich zu entschärfen ist. Oftmals erkennen Schutzlösungen diesen Traffic nicht als Anomalie.

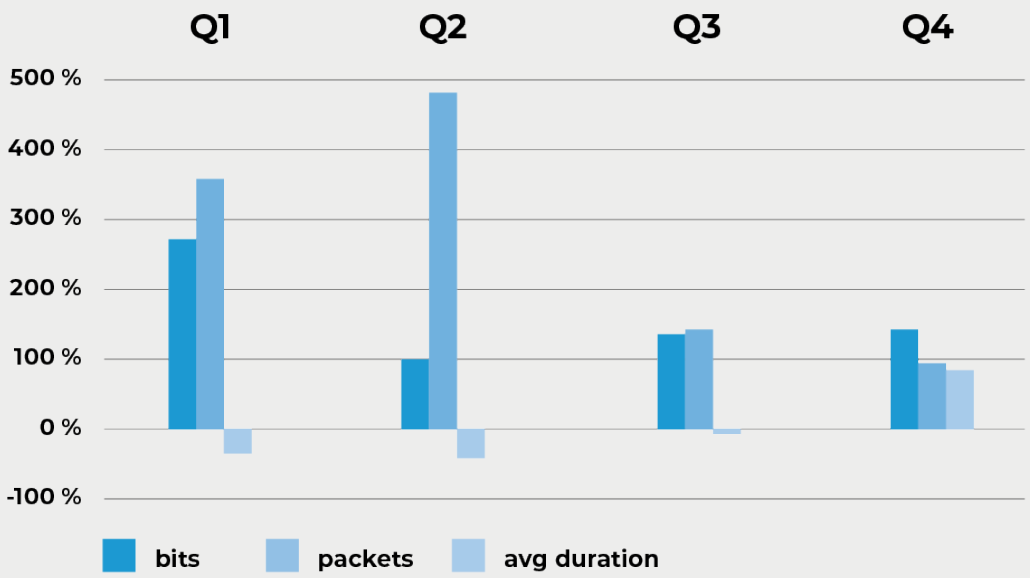
Die Zunahme der Intensität spiegelt sich jedoch nicht nur in der größer gewordenen durchschnittlichen Bandbreite wider, sondern auch in der Zunahme des Volumens hinsichtlich der Menge an den übertragenen Paketen. Während im Betrachtungszeitraum die durchschnittliche Anzahl der Paketrate bei 3,3 Millionen Paketen pro Sekunde lag, war die Paketrate im Jahr 2021 deutlich geringer. Im Angriffsfall wurden nur 990.000 Pakete pro Sekunde übermittelt.

Ein Blick auf die Korrelation zwischen Dauer und Intensität der DDoS-Angriffe offenbart besonders für das erste Halbjahr 2022 eine Veränderung: Die Angriffe waren intensiver und gleichzeitig kürzer. Dies zeigt, dass Zeit bei der Bekämpfung von DDoS-Angriffen eine immer wichtigere Rolle spielt. Wichtig ist, wie schnell auf den Angriff reagiert und mit der Schadensbegrenzung begonnen wird (Time-to-Mitigate) sowie wie lange es dauert, bis alles wieder normal läuft (Mean-Time-To-Repair). 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“.*

Bandbreiten-Peak pro Monat | 2021 vs 2022



Veränderung der Dauer und Intensität der Attacken



Wenn es um den Schutz vor immer konzentrierteren und anspruchsvolleren Angriffen geht, ist Präzision und Geschwindigkeit in der Erkennung und Abwehr von Angriffen besonders wichtig. Haben die Angreifer eine dieser anspruchsvollen und gefährlichen DDoS-Attacken gestartet, gibt es nur noch ein sehr enges Zeitfenster, um die potenziellen Schäden zu begrenzen. Denn besonders bei den schnell auftretenden und intensiven Attacken mit großen Bandbreiten sowie hohen Paketraten werden die Schutzlösungen auf die Probe gestellt.

Einige On-Premise-Systeme können einfache und unkoordinierte Angriffe abwehren. Primär deckt der Schutz vor allem netzwerkartige Angriffe (z. B. ICMP-UDP-Floods) auf Layer 3 oder 4 ab, jedoch können komplexere und besonders intensive Angriffe die Geräte überfordern.

In einem solchen Szenario reicht bereits eine Time-to-Mitigate von lediglich einer Minute nicht aus, um einen kompletten Ausfall des Systems zu vermeiden. Stattdessen geht es darum, den Datenverkehr in Echtzeit mit einer cloudbasierten automatisierten KI-Technologie zu analysieren, um die DDoS-Angriffe innerhalb kürzester Zeit abzuwehren.

”

Eine schnelle TTM ist für Betreiber kritischer Infrastrukturen unverzichtbar und ein hybrides System kann den entscheidenden Vorteil bieten – aber nur, wenn es regelmäßig überprüft wird, um sicherzustellen, dass die Schutzlösungen auf allen Ebenen effektiv arbeiten.

Jag Bains, Vice President Solution Engineering, Link11

Multi-Vektor-Attacken

Multi-Vektor-Attacken werden komplexer

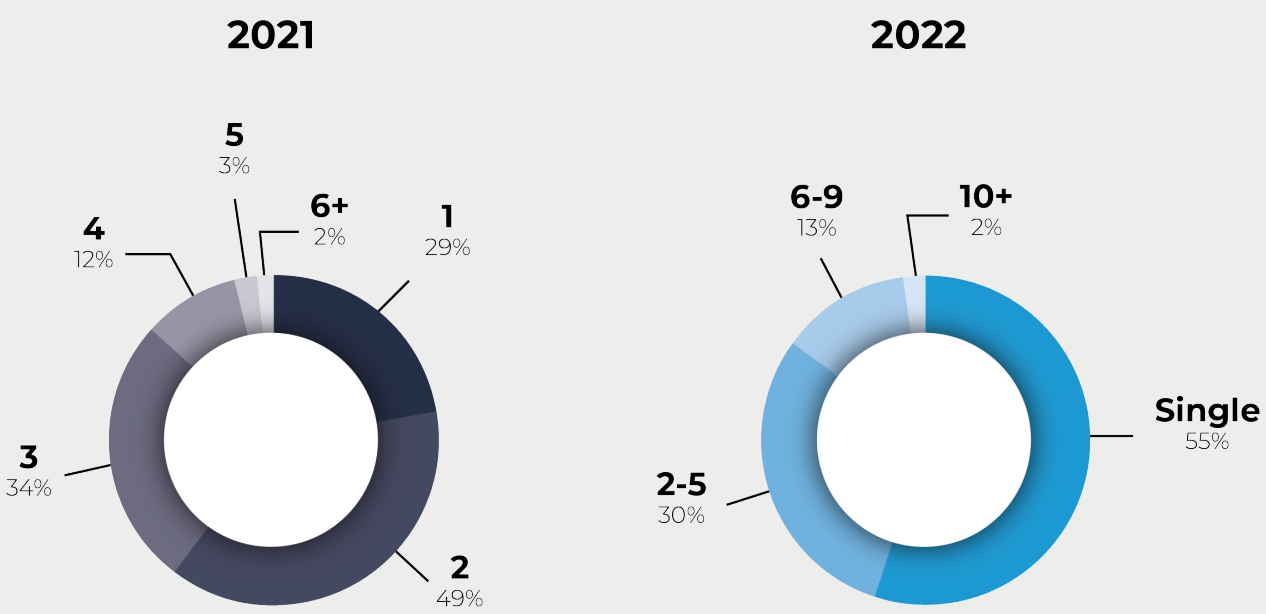
Multi-Vektor-Attacken sind eine besonders gefährliche Art von DDoS-Angriffen. Im Gegensatz zu herkömmlichen Angriffen, bei denen nur ein Angriffsvektor genutzt wird, richten sich Multi-Vektor-Angriffe parallel an mehrere Schwachstellen in den Bereichen Transport, Applikation und Protokoll. Durch den Einsatz mehrerer Angriffsvektoren wird es für die Verteidigungssysteme schwieriger, den Angriff zu erkennen und abzuwehren.

Die Kombination mehrerer Techniken steigert die Erfolgswahrscheinlichkeit für Angreifer, da viele Schutzlösungen nicht auf dem neuesten Stand sind. Es ist daher wichtig, Schutzlösungen zu nutzen, die effektiv gegen Multi-Vektor-Attacken auf allen Filter-Ebenen arbeiten.

Im ersten Halbjahr 2022 hat der Anteil der Multi-Vektor-Angriffe im Vergleich zum Vorjahr abgenommen. Während 2021 der Anteil von Multi-Vektor-Attacken bei 71 % lag, waren in den ersten sechs Monaten nur rund ein Drittel der Attacken (35 %) multidimensionale Angriffe.

Um sich vor Multi-Vektor-Attacken zu schützen, ist es ratsam, eine spezialisierte DDoS-Schutzlösung zu implementieren, die eine kontinuierliche Überwachung und Abwehr von Angriffen gewährleistet. Ein solches System kann Angriffe in Echtzeit erkennen und abwehren, um das Risiko einer längeren Downtime zu minimieren.

Anzahl der Single- und Multi-Vektor-Angriffe | 2021 vs 2022

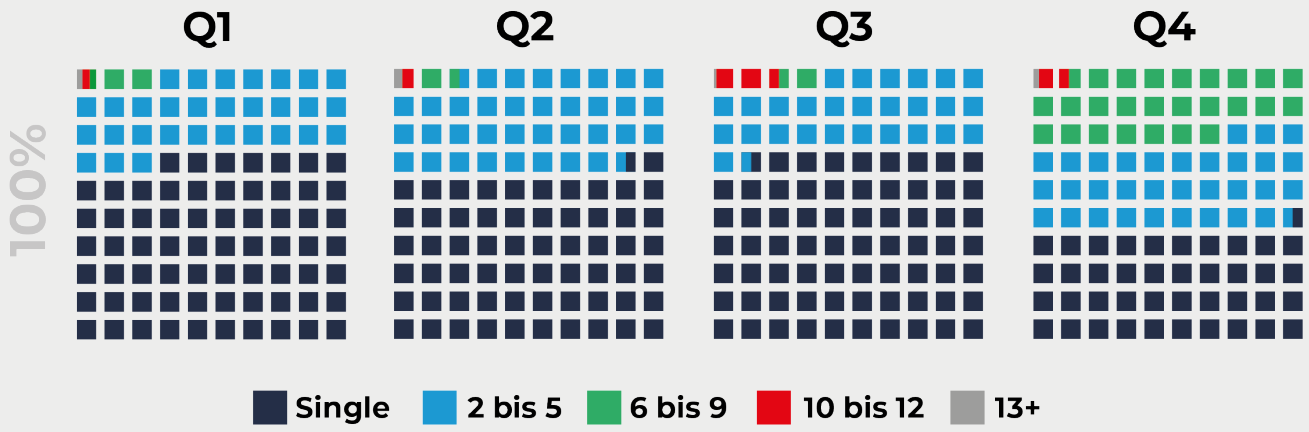


Diese Entwicklung hat sich im zweiten Halbjahr 2022 nicht fortgesetzt. Stattdessen haben Multi-Vektor-Attacken in der zweiten Jahreshälfte zugenommen. Insgesamt ist der Anteil der Multi-Vektor-Attacken von Juli bis Dezember 2022 auf 45 % gestiegen, wobei der deutlichste Anstieg im 4. Quartal zu erkennen ist.

Die höchste Anzahl an im Link11-Netzwerk beobachteten gleichzeitig eingesetzten Vektoren betrug 18. Dies sind bisher die größten im Netzwerk von Link11 beobachteten Multi-Vektor-Attacken gewesen. Im Jahr 2021 betrug die Anzahl gleichzeitig eingesetzter Vektoren 12.

Ein Angriff mit 18 verschiedenen Vektoren kann deutlich größeren Schaden verursachen. Multi-Vektor-DDoS-Attacken zeichnen sich durch ihre Fähigkeit aus, gleichzeitig mehrere Schwachstellen in einem System zu attackieren. Dadurch kann die Last auf die IT-Systeme enorm zunehmen, was zu einer Überlastung und letztlich zu einer längeren Downtime, im schlimmsten Fall zu einem kompletten Ausfall führen kann.

Veränderung der Single- und Multi-Vektor-Angriffe 2022



Hinkt die IT-Sicherheit der Bedrohungslandschaft hinterher, genügt bereits ein einzelner Vektor, der gezielt und konzentriert eingesetzt wird, um großen Schaden anzurichten.

Jag Bains, Vice President Solution Engineering, Link11

Reflection-Amplification-Angriffe

Neue Sicherheitslücken trotz bekannter Bedrohungen

Reflection-Amplification-Attacken sind Multi-Vektor-Angriffe, die sich auf das Ausnutzen falsch konfigurierter Server und Services im Internet verlassen. Statt das Ziel direkt anzugreifen, missbrauchen sie Dienste wie DNS oder NTP. Es gibt viele solcher Internetdienste, bei denen die Verifizierung des Absenders nicht unterstützt oder erforderlich ist. Indem ein Angreifer den Absender fälscht (auch als Spoofing bekannt), bringt er Dienste dazu, unerwünschte Antworten an ein Ziel zu senden (Reflection).

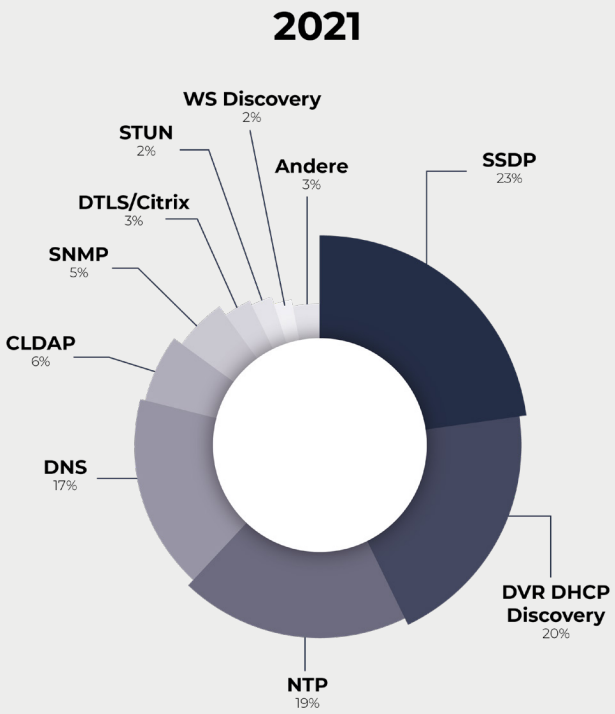
Dabei senden die Angreifer kleine Datenmengen an zwischengeschaltete Server, die als Verstärker dienen. In der Regel wählen Angreifer solche Dienste mit Antworten, die um ein Vielfaches größer sind als die eigentliche Anfrage. Somit erhöhen sie die Menge des gesendeten Datenverkehrs. Die missbrauchten Server spiegeln die Anfragen und leiten sie vielfach verstärkt (Amplification) an das eigentliche Angriffsziel weiter.

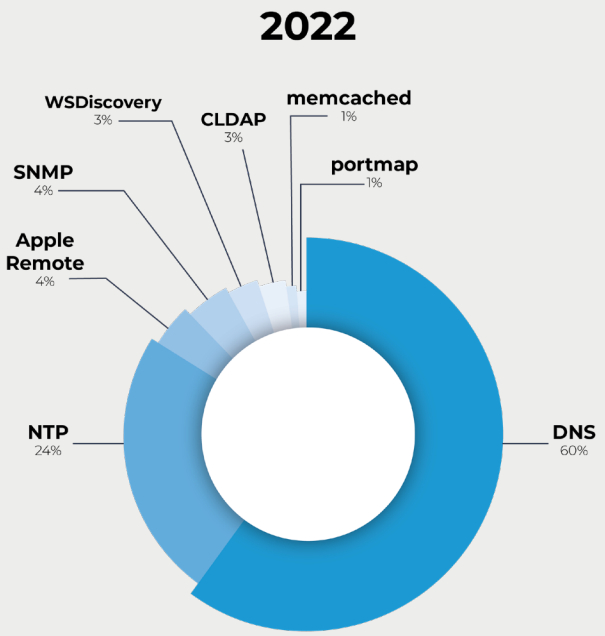
Im Jahr 2022 hat das LSOC eine Flut von Verstärkertechniken registriert. Viele dieser Angriffstechniken, wie DNS Reflection Amplification und NTP Reflection Amplification, zählen bereits seit 2013 zur Standard-Ausrüstung von DDoS-Angreifern. Diese Techniken zeichnen sich durch eine immense Verstärkung aus, beispielsweise durch eine 100-fache Verstärkung bei DNS-Attacken und eine bis zu 200-fache Verstärkung bei NTP-Angriffen.

Angreifer entdecken ständig neue Schwachstellen wie unzureichend geschützte Internetdienste und offene Dienste. Gleichzeitig wurden im Betrachtungszeitraum für die meisten Angriffe bereits bekannte und altbewährte Vektoren eingesetzt. Der Internetdienst, der 2022 am häufigsten für Angriffe ausgenutzt und als Verstärker missbraucht wurde, war DNS (60 %) gefolgt von NTP (24 %), SNPM (4 %) und Apple Remote (4 %).

Im Jahr 2022 war ein starker Anstieg der Popularität von DNS und NTP zu beobachten, die als Verstärkungsfaktor eingesetzt wurden. DNS ist eines der ersten und häufigsten genutzten Protokolle für diese Form der Angriffe.

Die wichtigsten Reflection-Amplification-Vektoren
2021 vs 2022





Das NTP (Network Time Protocol) wird verwendet, um Computeruhren über das Internet zu synchronisieren. NTP wurde erstmals vor rund zehn Jahren eingesetzt und ist aufgrund des großen potenziellen Verstärkungsfaktors nach wie vor sehr leistungsfähig. Innerhalb von NTP gibt es eine Funktion, mit der die letzten 600 Hosts, die das System abgefragt haben, zurückgegeben werden. Diese Reaktion kann bis zu 200-mal größer sein als die Anfrage, die sie erzeugt hat. Das bedeutet, dass ein Angreifer 1 Gbit/s an gefälschten Anfragen senden kann und die NTP-Server dem Ziel bis zu 200 Gbit/s unerwünschte Antworten senden werden.

Im Vergleich zum Vorjahr spielen hingegen das Simple Service Discovery Protocol (SSDP), das für die Erkennung von Plug-and-Play-Geräten verwendet wird und das Connectionless Lightweight Directory Access Protocol (CLDAP), ein verbindungsloses Verzeichnisprotokoll, keine große Rolle mehr.

Angreifer nutzen ständig neue Schwachstellen in Internetdiensten und ungeschützte Systeme für DDoS-Attacken aus. 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.

Einer der größten Verstärkungsfaktoren ist mit einer 50.000-fachen Verstärkung Memcached. Es gibt jedoch einen neuen TCP-Middleware-Angriff, der unter bestimmten Umständen das Potenzial hat, dies zu übertreffen. Theoretisch zeigte eine Forschungsarbeit im August 2021, dass mit dieser Verstärkungstechnik Angreifer Middleboxen wie Firewalls über TCP missbrauchen können, um Denial-of-Service-Angriffe zu verstärken. Die Forscher identifizierten zudem Hunderttausende IP-Adressen, die Angriffe mithilfe von Firewalls und Inhaltsfiltern um das Hundertfache verstärken.[33]

Eine gut funktionierende DDoS-Schutzlösung ist unverzichtbar, da die Angriffe immer fortgeschrittener werden und sich ständig weiterentwickeln. Unternehmen müssen sicherstellen, dass ihre Schutzmaßnahmen regelmäßig aktualisiert werden, um den neuesten Bedrohungen begegnen zu können. Ein guter Schutz bedeutet, schnell reagieren zu können, um Angriffe zu erkennen und innerhalb kürzester Zeit zu entschärfen.

”

Die Angriffsmethoden entwickeln sich weiter und die Cyberkriminellen können immer ausgeklügeltere Verstärkungstechniken in ihr Repertoire aufnehmen. Mit cloudbasierten und automatisierten DDoS-Schutzlösungen können Unternehmen damit Schritt halten.

Jens-Philipp Jung, Geschäftsführer, Link11

Ausblick

Cyberkrieg: DDoS-Attacken als strategisches Mittel

DDoS-Angriffe auf kritische Infrastrukturen werden im Rahmen der Cyberkriegsführung[34] immer häufiger vorkommen. Im Gegensatz zu konventionellen Kriegen kommen in einem Cyberkrieg digitale Waffen wie Viren, Malware oder DDoS-Angriffe zum Einsatz. Da überall zunehmend mehr Informationstechnologien genutzt werden, gewinnt diese Art Kriege zu führen immer mehr an Bedeutung.

Die zum Teil kosteneffizienten Cyber-Angriffe reichen von der Zerstörung von Computernetzen bis hin zur Unterbrechung von Energie- und Verkehrssystemen. Ziel ist es, die Infrastruktur eines Landes oder Unternehmens zu beschädigen oder lahmzulegen. Seit dem Einmarsch in die Ukraine wurden dort und in verschiedenen NATO-Ländern Angriffe auf Bereiche wie Energie, Banken und Finanzen sowie Gesundheit verzeichnet.

Die Gefahr für deutsche Unternehmen ist groß, wenn Hacker kritische Infrastrukturen angreifen. Obwohl es schwer ist, dass diese Angriffe tatsächlich die Kontrollsysteme erreichen, sind die jüngsten Angriffe ein besorgniserregendes Zeichen. Sie beweisen, dass russische Hackergruppen in den Diensten des Militärs oder Geheimdienstes bereit sind, kritische Infrastrukturen anzugreifen. Mit der zunehmenden Digitalisierung und weiter eskalierenden geopolitischen Konflikten ist ein Ansteigen dieser Angriffe zu erwarten.

Kopf-an-Kopfrennen zwischen Hackern und Verteidigern

Volumetrische DDoS-Angriffe, eine der weitverbreiteten Angriffsvarianten, haben an Effizienz im Infrastrukturbereich verloren. Das liegt daran, dass die Angriffe, die ein Netzwerk ausschließlich mit sehr viel Bandbreite überfluten, leicht von herkömmlichen DDoS-Schutzmaßnahmen erkannt und abgewehrt werden können. Dennoch bleibt die Bedrohungslage besonders für Betreiber kritischer Infrastrukturen durch politisch motivierte Angriffe hoch.

In der ersten Jahreshälfte 2022 wurden die weltweit größte Darknet-Plattform „Hydra-Market“ und Anbieter von „Booter-Diensten“, die DDoS-as-a-Service anbieten, abgeschaltet. Kurzfristig wird das die Zahl der Angriffe verringern. Die Nachfrage nach DDoS-Angriffen steigt jedoch weiter an. Daher ist es nicht die Frage, ob, sondern nur wann kriminelle Akteure neue Plattformen etablieren und sich eifrig einen neuen Namen machen.

Immer mehr Angreifer nutzen zunehmend künstliche Intelligenz, um ihre Methoden und Angriffstypen zu verbessern. Das führt dazu, dass sich der Wettlauf zwischen Angreifern und Verteidigern verschärft. Intelligente und robuste DDoS-Schutzlösungen wie die KI-gestützte, Ccloud-basierte 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 von 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 sicherer.

Verschärfte Cyber-Sicherheitsstandards durch neue Richtlinien

Gesetzgeber weltweit verschärfen die Cyber-Sicherheitsstandards und fordern die vollständige Offenlegung von Sicherheitsvorfällen unter Androhung harter Strafen. Am 16. Januar trat ein neues EU-Gesetzespaket[35] in Kraft. Die überarbeitete „EU Network and Information Security Directive“[36] kurz NIS2-Richtlinie soll das gemeinsame Sicherheitsniveau von Netz- und Informationssystemen in der EU erhöhen.

Wie schon die erste EU-weite Gesetzgebung im Bereich Cybersicherheit NIS soll NIS2 insbesondere kritische Infrastrukturen vor Hackerangriffen schützen. Die Richtlinie zielt darauf ab, auch das Management stärker in die Verantwortung zu nehmen. Allerdings könnte es für viele deutsche Unternehmen schwierig werden, die Vorgaben bis Herbst 2024 einzuhalten, da die Anforderungen erheblich sind.

Die Regulierung durch die NIS2-Richtlinie der EU richtet sich nach bestimmten Größenkriterien bei Unternehmen. Mittelgroße Firmen ab 50 Mitarbeiter und einem Umsatz von 10 Millionen Euro sowie große Unternehmen mit 250 Mitarbeitern und einem Umsatz von 50 Millionen Euro sind von der Regulierung betroffen.

Kleine und Kleinstunternehmen sind normalerweise von den Regulierungen nicht betroffen, aber einige ausgewählte Unternehmen können dennoch verpflichtet werden, die Cyber-Sicherheitsrisiken in ihren Lieferketten zu berücksichtigen. Es wird geschätzt, dass 80 % der Unternehmen nicht wissen, dass sie von „NIS2-Richtlinie“ betroffen sind.

Besonders strenge Vorgaben gelten für Sektoren mit hoher Kritikalität wie Energieversorger, Verkehrsunternehmen, Internet- und Cloud-Anbieter, Banken, Gesundheitsdienstleister und Organisationen aus dem Bereich Weltraum sowie die öffentliche Verwaltung. Parallel dazu führt die EU auch den „Cyber Resilience Act“ ein, der Vorgaben für die Gestaltung von Produkten „mit digitalen Elementen“ wie Hard- und Software enthält.

Der Entwurf für die NIS2-Richtlinie der EU beinhaltet genaue Regelungen über Meldepflichten, die mit hohen Strafen von mehreren Millionen Euro geahndet werden können. Auch in Kanada[37] wird eine Gesetzgebung geplant, die dem europäischen Datenschutz-Modell (DSGVO) nachempfunden ist und ähnliche Strafen vorsieht.

Die EU begründet ihre Initiative damit, dass die digitale Infrastruktur ein wichtiger Teil des Alltags und des grenzüberschreitenden Austauschs geworden ist und daher Cybersicherheit wichtiger denn je für den reibungslosen Betrieb des Binnenmarkts ist.

Nachweise

[1] https://www.bitkom.org/Presse/Presseinformation/Corona-hat-Bueros-dauerhaft-digitaler-gemacht

[2] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

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

[4] https://zero.bs/ddos-as-attackvector-for-state-sponsoredhacktivist-groups-in-times-of-crisis.html#evolution_of_killnet

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

[6] https://www.nbip.nl/en/news/ddos-attacks-q4-2022/?utm_campaign=General&utm_content=LinkedIn&utm_medium=social&utm_source=LinkedIn

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

[8] https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220405_PM_IllegalerDarknetMarktplatz.html

[9] https://www.zdnet.de/88405934/fbi-zerschlaegt-ddos-bande/

[10] https://www.golem.de/news/ddos-angriff-auf-minecraft-spieler-legt-internet-in-andorra-lahm-2201-162654.html

[11] https://www.zdnet.com/article/ukraine-ministry-of-defense-confirms-ddos-attack-state-banks-loses-connectivity/

[12] https://www.cshub.com/attacks/news/iotw-ukraine-suffers-15-hour-internet-outage

[13] https://www.bleepingcomputer.com/news/security/russian-hacktivists-launch-ddos-attacks-on-romanian-govt-sites/

[14] https://www.faz.net/aktuell/rhein-main/hessische-polizei-nimmt-website-nach-ddos-attacken-vom-netz-17994484.html

[15] https://www.heise.de/news/DDoS-Attacken-bei-E-Mail-Dienst-Anbieter-Posteo-7098580.html

[16] https://www.inside-it.ch/ddos-attacke-auf-eurovision-song-contest-wurde-abgewehrt-20220516

[17] https://www.tagesschau.de/inland/cyberattacke-bundesregierung-ddos-101.html

[18] https://www.hackread.com/pro-iran-altahrea-hit-port-of-london-website-ddos-attack/

[19] https://thebarentsobserver.com/en/security/2022/06/pro-russian-hacker-group-says-it-attacked-norway

[20] https://cryptoslate.com/tether-confirms-ddos-attack-on-tether-io/

[21] https://www.wa.de/hamm/internet-nur-noch-im-schneckentempo-massive-cyber-attacke-auf-die-helinet-in-hamm-91656377.html

[22] https://edition.cnn.com/2022/07/08/politics/congress-website-disrupted/index.html

[23] https://www.ndr.de/nachrichten/niedersachsen/oldenburg_ostfriesland/Oldenburg-Cyberattacke-auf-Gesellschaft-von-EWE,aktuelloldenburg10302.html

[24] https://www.nbcnews.com/tech/security/taiwanese-websites-hit-ddos-attacks-pelosi-begins-visit-rcna41144

[25] https://www.n-tv.de/ticker/Irans-Zentralbank-bestaetigt-DDos-Attacke-article23603881.html

[26] https://www.pokernews.com/news/2022/09/pokerstars-ddos-attack-caused-wcoop-outage-rescheduled-42164.htm

[27] https://www.securityweek.com/us-airport-websites-hit-suspected-pro-russian-cyberattacks

[28] https://insideparadeplatz.ch/2022/11/09/black-tuesday-fuer-trading-bank-swissquote/

[29] https://www.bleepingcomputer.com/news/security/pro-russian-hacktivists-take-down-eu-parliament-site-in-ddos-attack/

[30] https://www.bleepingcomputer.com/news/security/massive-ddos-attack-takes-russia-s-second-largest-bank-vtb-offline/

[31] https://futurezone.at/digital-life/oebb-oebb-website-down-stoerung-hacker-ddos/402261678

[32] https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/killnet
https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/
https://www.darkreading.com/ics-ot/killnet-pro-russia-hacktivist-group-support-influence-grows

[33] https://www.usenix.org/conference/usenixsecurity21/presentation/bock

[34] https://www.enisa.europa.eu/news/volatile-geopolitics-shake-the-trends-of-the-2022-cybersecurity-threat-landscape

[35] 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/

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

[37] https://www.torys.com/our-latest-thinking/publications/2022/12/data-protection-enforcement

Kontakt

Link11 GmbH
Lindleystr. 12
60314 Frankfurt