LINK11

DDOS-REPORT

für das Jahr 2021

Inhalt

Einleitung und Zusammenfassung

Unsere Lebenswelt wird immer digitaler. Das gilt für den privaten Raum genauso wie für Wirtschaft und Industrie. Mit der weltweiten Vernetzung über Unternehmens- oder Ländergrenzen hinweg nimmt gleichzeitig die **Cyberkriminalität** rasant zu. Es werden Daten gestohlen, IT-Systeme lahmgelegt und Lösegeld verlangt. Im Oktober 2021 hat das **Bundesamt für Sicherheit in der Informationstechnik** (BSI) aufgrund steigender Gefahren durch Cyberattacken die **Alarmstufe rot** ausgerufen. Auch der Digitalverband Bitkom ist beunruhigt, da die Cyberattacken nicht nur internationaler, sondern auch immer professioneller werden. Besonders für Unternehmen gehören Cybergefahren zu den größten Risiken. Der Schaden allein für die deutsche Wirtschaft liegt laut einer im August 2021 veröffentlichten **Bitkom-Cybersicherheitsstudie** bei mehr als **220 Milliarden Euro**. Als zweitgrößte Gefahr nach der Infizierung mit Malware haben **DDoS-Attacken** bei 27 % der Unternehmen einen Schaden verursacht. Tendenz steigend. [1]

> Die Intensität und Aggressivität der Erpressungen ist nach Einschätzung der IT-Sicherheitsexperten von Link11 noch einmal spürbar gestiegen.

In dem weiterhin durch die Corona-Pandemie geprägten Jahr 2021 verzeichnete das Link11 Security Operation Center (LSOC) für das Gesamtjahr einen Anstieg in der Anzahl der Attacken von 41 % im Vergleich zum Vorjahr und hat damit gegenüber dem Anstieg von 33 % im Vergleich der Halbjahreszeiträume H1 2020 zu H1 2021 nochmals zugelegt. Dabei haben **Hochvolumen-Attacken** signifikant zugenommen. Der durchschnittliche Bandbreiten-Peak lag in den vergangenen zwölf Monaten bei 437 Gbps. Die höchste im Link11-Netzwerk gemessene Angriffsbandbreite lag über 1 Tbps und summierte sich in knapp 2 Stunden auf über 4,5 Tbps Volumen auf den gleichen Kunden. Gleichzeitig entwickelten sich die sogenannten **„Carpet Bombing“**-Angriffe zu einer großen Herausforderung für Hosting- und Cloud-Anbieter, ISPs und Carrier. Bei diesen technisch sehr komplexen Angriffen ist der Datenverkehr pro IP-Adresse im Gegensatz zu den Hochvolumen-Attacken so gering, dass viele Schutzlösungen sie nicht als Anomalie erkennen. Die Angriffe fliegen oft unter dem Radar und sind schwer zu entschärfen. Hinzu kommt, dass der Angreifer den DDoS-Verkehr nicht auf ein bestimmtes System oder einen Server lenkt. Es wird nicht nur eine IP-Adresse angegriffen, sondern ein ganzer Netzwerkblock mit mehreren hundert oder tausend Adressen.

Neben den Angriffen unter dem Radar sind auch komplexe **Multivektor-Attacken** weiter auf dem Vormarsch. Multivektor-Angriffe zielen parallel auf Schwachstellen in Transport-, Applikations- und Protokollebene. Je mehr Schwachstellen und Protokolle Angreifer bei einem Angriff missbrauchen, umso schwieriger ist die Angriffserkennung und Abwehr. Der Anteil dieser Methodik ist von 59 % im Jahr 2020 auf 71 % im Jahr 2021 gestiegen. Damit haben die Multivektor-Attacken einen neuen Höchststand erreicht.

Daneben verstärkte sich 2021 **Ransom-DDoS** als Trend: Immer mehr Cyberkriminelle fordern bei DDoS-Attacken zunehmend Lösegeld. Die Intensität und Aggressivität der **Erpressungen** ist nach Einschätzung der IT-Sicherheitsexperten von Link11 noch einmal spürbar gestiegen. Das Ausmaß übertrifft die vielen cyberkriminellen DDoS-Aktivitäten, die bislang beim Schutz der zahlreichen Kunden in den vergangenen Jahren beobachtet wurden, bei Weitem. Während einer Angriffsserie auf VoIP-Anbieter in Nordamerika verlangten die Angreifer Lösegeld in Höhe von bis zu 4,5 Millionen Dollar in **Bitcoins**. Verstärkend auf diesen Trend könnte sich nach Einschätzung von Link11 die Tatsache auswirken, dass **DDoS-Attacken** im vergangenen Jahr oftmals auch als **Nebelkerzen** zum Einsatz kamen. Im Windschatten eines massiven DDoS-Angriffs können die Hacker unbemerkt durch die Hintertür in die Netzwerksicherheit eindringen und angreifen. DDoS-Angriffe verändern die Datenverkehrsprofile drastisch und erzeugen ein Rauschen, das zum Beispiel einen **Datendiebstahl** verschleiert, der das eigentliche Ziel dieser Angriffe ist. Umso wichtiger ist eine umfassende und gezielte Risikoanalyse, um die richtigen Sicherheits-Tools zu identifizieren.

DDoS in den Nachrichten

1. Halbjahr

30. Januar 2021

Digitales Fernsehen in Island nicht erreichbar

Das Streaming-TV-Angebot des isländischen Telekommunikationsanbieters Siminn war an einem Samstagabend und noch dazu in der Pandemie nicht erreichbar. Nach ca. zwei Stunden war der DDoS-Angriff gestoppt und der Service wieder erreichbar. [2]

18. Februar 2021

Österreichweite Internet-Ausfälle

Beim Festnetzinternet des Telekommunikationsanbieters A1 kam es zu einem zweistündigen Ausfall im ganzen Land, was in Pandemiezeiten im Home-Office problematisch war. Schuld waren DDoS-Attacken, die zu einem Routing-Problem geführt hatten. [4]

4. Mai 2021

Staatliche Einrichtungen in Belgien offline

Dienste und Webseiten von mehr als 200 staatlichen Organisationen und Institutionen in Belgien waren mehrere Stunden digital nicht erreichbar. Auslöser waren Angriffe auf den ISP Belnet, der u. a. das Netzwerk für die belgische Regierung bereitstellt. [6]

9. Juni 2021

Großflächige Stromausfälle in Puerto Rico

Im Karibikstaat gingen bei gut 700.000 Einwohnern die Lichter aus, nachdem erst eine DDoS-Attacke den Energieversorger getroffen hatte und nur wenige Stunden später ein Umspannungswerk in Flammen aufging. [8]

Januar – März 2021

Impfportale weltweit durch Angriffe gestört

In mehreren Ländern wie Großbritannien, Deutschland und den USA häuften sich Meldungen von Cyber-Angriffen auf Impfportale. Die Webseiten, die der Buchung von Impfterminen mit dem COVID-19-Impfstoff dienen, wurden mit DDoS-Attacken überlastet. [3]

8. März 2021

Parlamentswebseite in Italien offline

Die institutionelle Webseite der Abgeordnetenkammer, die mit dem Senat das italienische Parlament bildet, war über einen Tag nicht erreichbar. Die Täter hinter dem Angriff und ihr Motiv blieben unklar. [5]

18. Mai 2021

ISP in Irland im Visier

In der ersten Maihälfte wurden zahlreiche ISPs in Irland das Ziel von DDoS-Attacken. So wurde mit Blacknight einer der größten Web-Hosting-Anbieter des Landes angegriffen. Dabei kam es zu zahlreichen mehrstündigen Ausfällen. Die Angriffe wurden vielfach von DDoS-Erpressungen begleitet. [7]

DDoS in den Nachrichten

2. Halbjahr

September – November 2021

Angriffsserie auf internationale VoIP-Anbieter

Zwischen September und November wurden mehrere internationale VoIP-Anbieter angegriffen. Darunter auch die international agierenden Branchengrößen Bandwidth, VoIP.ms und Telnyx. Tagelang legten die Angriffe die Dienste der Service Provider lahm. Die Hacker-Gruppe REvil verantwortete einen Großteil der Angriffe und forderte Lösegelder in Höhe von bis zu 4,5 Millionen Dollar. [9]

12. September 2021

Meris-Botnetz Rekordangriff lähmt russischen Internetgiganten

Der russische Internetgigant Yandex war Ziel eines massiven DDoS-Angriffs mit bis zu 21,8 Millionen Anfragen pro Sekunde. Initiiert wurde der bisher größte Angriff auf das russische Internet RuNet vom neuartigen Botnetz Meris. Vermutungen zufolge stammten die Anfragen von bis zu 250.000 kompromittierten Rechnern mit Ethernet-Anschluss. [10]

13. September 2021

Kein Onlinebanking in Neuseeland

Zu den Opfern eines breit angelegten DDoS-Angriffs gehörten neuseeländische Banken, der landesweite Wetterdienst sowie die Post und die Polizei des Landes. Über Tage hinweg kam es zu Zugangsproblemen, Ausfällen des Internetbankings und Problemen bei Kartenzahlungen. [11]

8. Oktober 2021

Bildungsportale in der Schweiz tagelang offline

Der gezielte und massive Angriff auf die IP-Adressen traf das Schweizerische Dienstleistungszentrum Berufsbildung (SDBB) mit voller Wucht. Fast zwei Wochen lang waren mehrere Bildungsplattformen in der Schweiz nicht erreichbar. [12]

23. November 2021

Alternative spanische Medien Opfer gezielter Hackerangriffe

Die spanischen Alternativmedien La Marea und El Salto wurden Opfer einer Hackerkampagne gegen linke und alternative Medien, die bereits Mitte November startete. Die Webseiten brachen unter dem DDoS-Angriff vom Typ L7, bei dem die Seitenzugriffe enorm erhöht werden, vollständig zusammen. [13]

15. Dezember 2021

Den Haags Computersysteme unerreichbar

Die Computersysteme der Stadt Den Haag wurden mit Datenverkehr so stark überlastet, dass die Dienste der Stadtverwaltung ausfielen. [14]

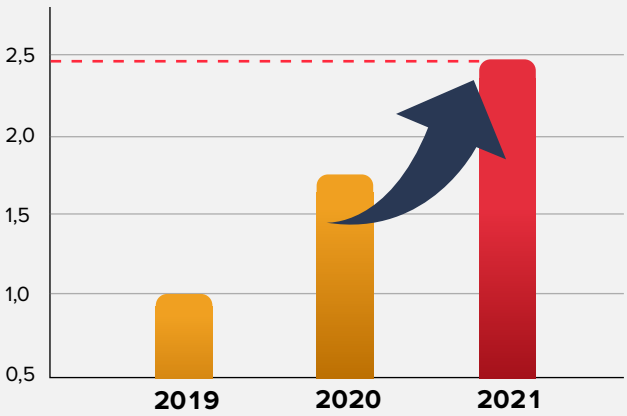
Entwicklung der Gesamtzahlen im Link11-Netzwerk

New Work, New Life und weiter steigende DDoS-Attacken

Seit Beginn der Corona-Pandemie findet ein Großteil unseres Lebens im Netz statt. Berufstätige weltweit haben mehrere Videokonferenzen die Woche. Allein Microsoft Teams wurde im April 2021 von 145 Millionen Menschen rund um den Globus genutzt. Das waren 113 Millionen mehr Menschen als noch im März 2020 [15]. Arbeiten über VPN-Zugänge im Homeoffice gehört bei vielen Firmen mittlerweile zum Standard und könnte sich nach Corona auf hohem Niveau stabilisieren. E-Learning, E-Commerce, E-Government – immer mehr Anwendungen und Dienste werden digital genutzt. Die Folgen: der Datenverkehr hat 2021 weiter zugenommen, wie der weltweit führende Internet-Knoten-Betreiber DE-CIX Frankfurt bekannt gab. Insgesamt sind mehr als 38 Exabyte Daten ausgetauscht worden, was einem Anstieg gegenüber dem Vorjahr von fast einem Fünftel (20 %) entspricht. Mit einem solchem Datenvolumen könnten rund 18.000 Menschen ihr Leben lang ein HD-Video streamen. [16]

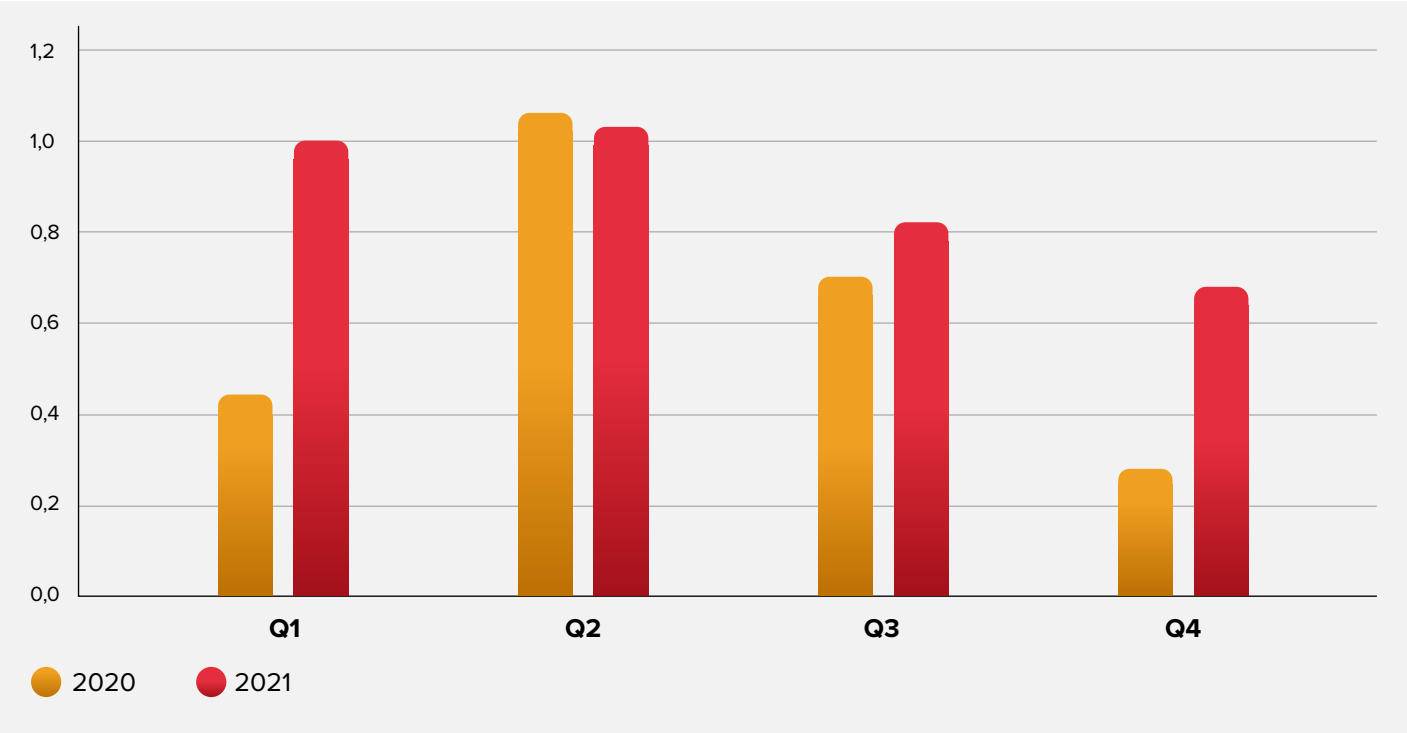
Es ist kein Zufall, dass in einer immer stärker vernetzten Welt die Angriffsflächen zunehmen und damit auch die DDoS-Attacken auf einen neuen Höchststand liegen. Im Jahresvergleich lag die Anzahl der Attacken, die im Netzwerk von Link11 registriert wurden, erneut deutlich über dem Vorjahreszeitraum. Die Zunahme 2021 gegenüber 2020 betrug insgesamt 41 %. Verglichen mit dem Vorjahreszeiträumen kam es im ersten Quartal 2021 zu mehr als doppelt so viel (108 %) und im vierten Quartal trotz eines

Relative Entwicklung DDoS Attacken 2019 – 2021



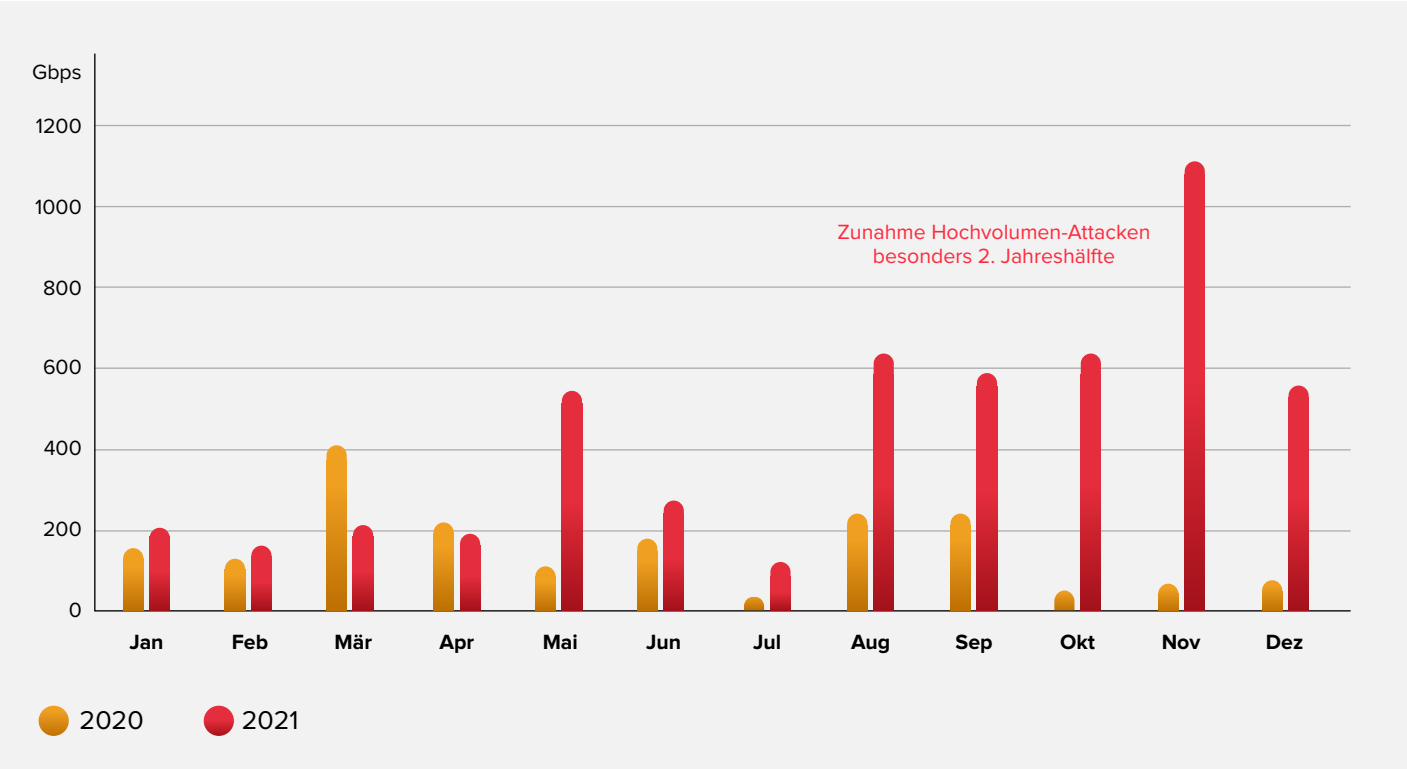
Rückgangs im Vergleich zum 1. Halbjahr zu fast 2,5-mal (148 %) mehr Angriffen als im gleichen Zeitraum 2020. Neben internationalen Hosting-Anbietern waren u.a. auch Banken, Impfportale, Lernplattformen sowie öffentliche Einrichtungen von DDoS-Angriffen betroffen. Dabei kam es auch zu deutlich mehr Ransom-DDoS-Angriffen und höheren Lösegeldforderungen. Dem Jahresbericht der europäischen Strafverfolgungsbehörde zur organisierten Internetkriminalität (IOCTA) zufolge, führten weiterentwickelte Techniken und die relativ einfache Umsetzung von DDoS-Attacken zu einem Anstieg der Lösegeldzahlungen um mehr als 300 % im Vergleich zu 2019 und 2020. [17]

Relative Anzahl DDoS Attacken Q1 – Q4, 2020 vs. 2021



Entwicklung der Angriffsbandbreiten

Bandbreiten-Peak pro Monat



Drastische Zunahme von Hochvolumen-Attacken

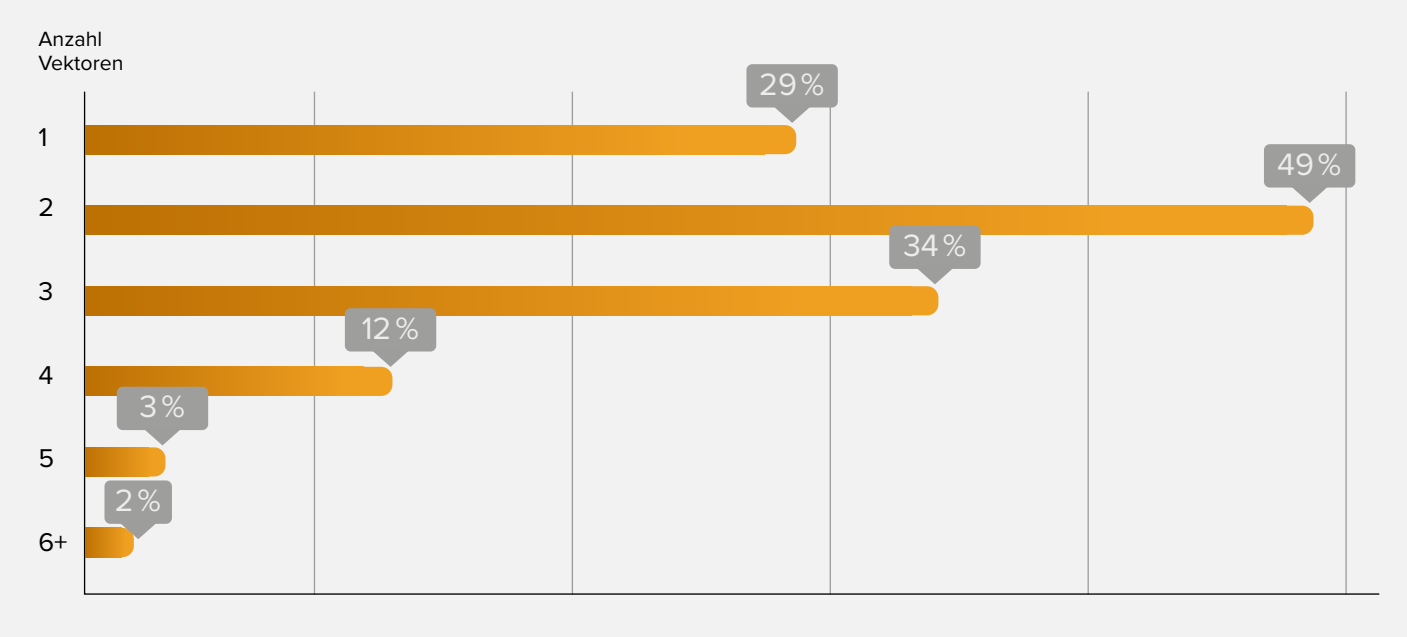
Hochvolumen-Attacken haben im Jahr 2021 signifikant zugenommen. In den vergangenen zwölf Monaten lag der durchschnittliche Bandbreiten-Peak bei 437 Gbps, während im Jahr 2020 die Angriffsbandbreite pro Monat durchschnittlich 161 Gbps betrug. In zehn von zwölf Monaten lag die Angriffsbandbreite der DDoS-Attacken über den Vergleichszahlen aus 2020. Die vom LSOC gemessenen Bandbreiten überschritten dabei jeden Monat die Marke von 100 Gbps. Besonders in der zweiten Jahreshälfte verzeichnete Link11 im Netzwerk zahlreiche Hochvolumen-Attacken. Zwischen August 2021 und Dezember 2021 schwankten die Bandbreiten der Hochvolumen-Attacken zwischen 546 Gbps und dem höchsten gemessenen Einzelausschlag von 1,1 Tbps. Verantwortlich für die Zunahme der Hochvolumen-Attacken war unter anderem das neue und massive Botnet Meris, das nach dem lettischen Wort für Pest benannt ist. Cybersicherheitsexperten gehen von rund 250.000 kompromittierten Geräten weltweit aus. Damit gelingt es Meris, auch sehr robuste Netzwerke durch eine große Anzahl von Anfragen pro Sekunde (RPS) zu stören. Anders als die alte Mirai-DDoS-Malware stützt sich Meris auf spezialisierte Module, die volumetrische Angriffe statt reine Bandbreitenangriffe starten. [18]

Dagegen ist die mittlere Gesamtbandbreite von 1,5 Gbps im Jahr 2020 auf 1,4 Gbps im Jahr 2021 aufgrund der Zunahme des sog. „Carpet-Bombings“ gesunken. Siehe dazu den Abschnitt „Carpet-Bombing“ auf Seite 13.

Nur eine hochleistungsfähige IT-Sicherheitslösung kann bei der Abwehr von DDoS-Angriffen leistungsfähiger Botnetze wie Meris helfen.

Multivektor-Attacken

Anteile der Single- oder Multivektor-Angriffe



Komplexe Multivektor-Attacken auf dem Vormarsch

In den vergangenen Jahren ist die Komplexität der DDoS-Attacken nach den Beobachtungen des LSOC zunehmend gewachsen. Es dominieren Multivektor-Angriffe mit mindestens zwei unterschiedlichen Angriffsvektoren. Diese zielen parallel auf Schwachstellen in Transport-, Applikations- und Protokollebene. Je mehr Schwachstellen und Protokolle Angreifer bei einem Angriff missbrauchen, umso schwieriger ist die Angriffserkennung und Abwehr. Alle einzelnen Vektoren müssen identifiziert werden, um ein Muster zu erkennen. Solche multidimensionalen Angriffe bedeuten daher, dass es sich praktisch um mehrere gleichzeitig laufende Attacken handelt. Deren Anteil ist von 59 % im Jahr 2020 auf 71 % im Jahr 2021 gestiegen und hat damit einen neuen Höchststand erreicht. Bei dieser Methodik, bei der die Angreifer mehrere Techniken kombinieren, steigt die Erfolgswahrscheinlichkeit für die Angreifer. Denn die am Markt verbreiteten Schutzlösungen sind oftmals nicht auf dem neuesten Stand, und deren Patch- und Updatezyklen hinken der Bedrohungslandschaft hinterher. Um die Unternehmens-IT zuverlässig abzusichern, ist es daher wichtig, auf Schutzlösungen zu setzen, die auf allen Filter-Ebenen von Multivektor-Attacken effektiv arbeiten. Nur noch bei knapp einem Drittel (29 %) der Attacken im Jahr 2021 setzten die Angreifer auf einen einzelnen Vektor. Die höchste Anzahl an im Link11-Netzwerk beobachteten gleichzeitig eingesetzten Vektoren betrug 12.

> **Multivektor-Angriffe zu bekämpfen, gleicht dem Kampf gegen die Hydra: Entschärft man einen Vektor, stellt man fest, dass er durch zwei weitere ersetzt wird. Halten Sie in Zukunft Ausschau nach noch vielfältigeren und komplexeren Multivektor-Angriffen und bereiten sie sich bestmöglich darauf vor.**
>
> **– Jag Bains,** Vice President Solution Engineering, Link11

Reflection-Amplification-Angriffe

Was sind Reflection-Amplification-Angriffe?

Reflection-Amplification-Angriffe sind eine Klasse von Multivektor-Angriffen, die verschiedene falsch konfigurierte offene Server und Services im Internet auf ähnliche Art ausnutzen. Dabei wird das Zielsystem nicht direkt angegriffen, sondern es werden dazu Dienste wie DNS oder NTP missbraucht. Der Angreifer sendet dabei zunächst kleine Mengen von Datenpaketen an die zwischengeschalteten Server, die als Verstärker dienen: Sie spiegeln die Anfragen (reflection) und leiten sie vielfach gesteigert (amplification) an das eigentliche Angriffsziel weiter. Die Steigerung liegt dabei zwischen 24-facher Verstärkung bei DVR DHCP Discovery-Angriffen und 100-facher Verstärkung bei DNS-Attacken sowie bis zu 200-facher Verstärkung bei NTP-Angriffen.

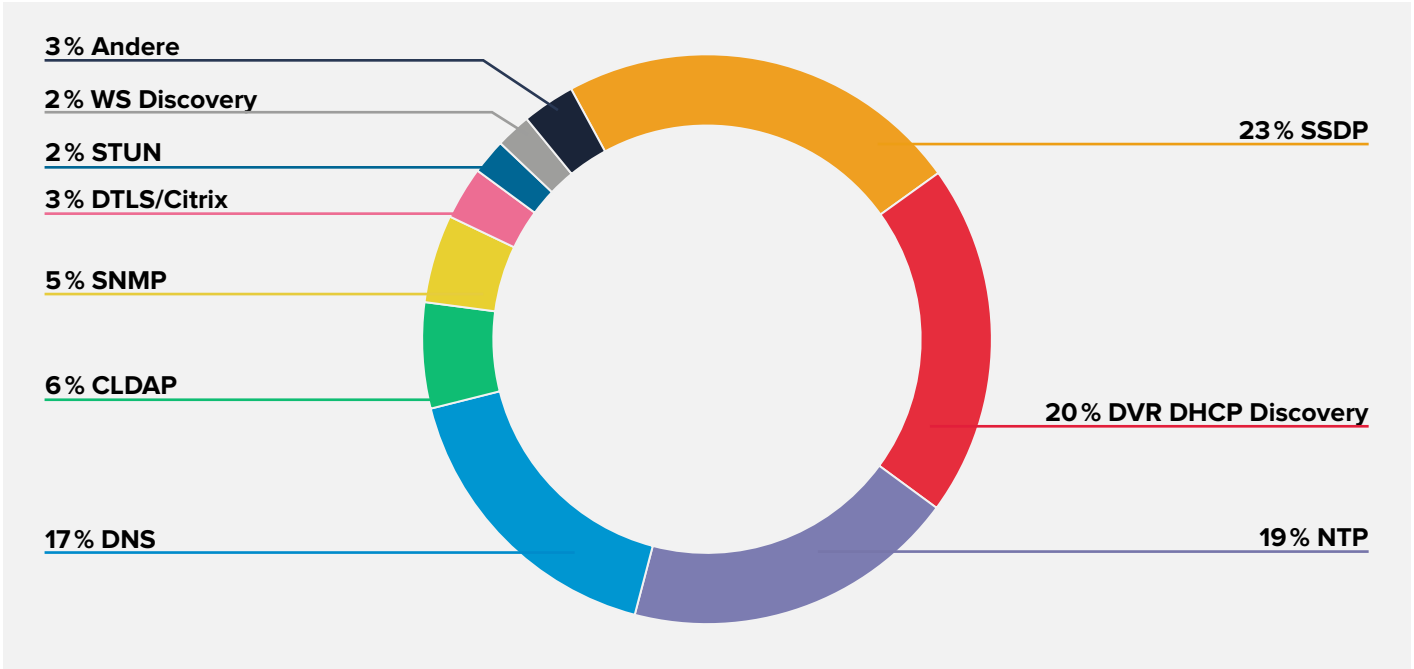
Neue Vektoren treten auf den Plan

Die ersten Reflection-Amplification-Vektoren traten im Jahr 2013 auf und betrafen DNS und NTP. Seitdem ist das Spektrum der Vektoren weitaus größer geworden. Derzeit gibt es über 20 Techniken, darunter Memcached-Reflection-Amplification und CLDAP. Im ersten Halbjahr 2021 hat das LSOC neue Vektoren über sein globales Netzwerk und seine KI-basierte Mitigation-Technologie identifiziert: Datagram Transport Layer Security (DTLS) über Citrix Netscaler und Session Traversal Utilities for NAT (STUN). DTLS wurde entwickelt, um verschlüsselte Daten nicht nur über gesicherte, verbindungsorientierte Transportprotokolle wie TCP, sondern auch über das verbindungslose UDP übertragen zu können. Ein STUN-Server sorgt dafür, dass Endgeräte wie Computer oder VoIP-Telefone, die sich im lokalen Netzwerk hinter einem Router oder einer Firewall verbergen, mit VoIP-Providern im Internet kommunizieren können. Angreifer entdecken ständig neue Schwachstellen wie unzureichend geschützte Internetdienste und offene Dienste. Gleichzeitig wurden 2021 für die meisten Angriffe bereits bekannte und altbewährte Vektoren eingesetzt. Der Internetdienst, der 2021 am häufigsten für Angriffe ausgenutzt und als Verstärker missbraucht wurde, war SSDP (23 %) gefolgt von DVR DHCP Discovery (20 %), NTP (19 %) und DNS (17 %).

Anfang des Jahres waren DVR-DHCP-Discovery-Angriffe die am weitesten verbreiteten Reflection-Amplification-Angriffe. Dieses Protokoll wird für die Netzwerkverwaltung von DVR-Recordern verwendet. Im zweiten Quartal war DNS das wichtigste Protokoll für Amplification-Angriffe. DNS ist eines der ersten und häufigsten genutzten Protokolle für diese Form der Angriffe. SSDP und NTP verursachten in der zweiten Jahreshälfte die meisten Reflection-Amplification-Angriffen. Das Simple Service Discovery Protocol wird für die Erkennung von Plug-and-Play-Geräten verwendet. Das Network Time Protocol wird für die Zeitsynchronisation zwischen Geräten verwendet.

Obwohl deren Missbrauchspotenzial schon so lange bekannt ist, werden die Sicherheitslücken nur unzureichend gepatcht. Umso wichtiger ist es, sich zu versichern, ob die eingesetzte DDoS-Schutzlösung generell in der Lage ist, neue, bisher unbekannte Angriffsvektoren zu erkennen und innerhalb weniger Sekunden zu entschärfen.

Top 10 Reflection-Amplification-Vektoren



Mehrere Wellen von DDoS-Erpressungen und Datendiebstahl

Lösegeldangriffe haben 2021 weiter zugenommen

Seit Anfang des Jahres 2021 sorgten zudem wiederholte und sich immer weiter verstärkende Wellen von DDoS-Erpressungen für eine angespannte Gefahrenlage. Erpresser-Mails mit wechselnden Absendern wie Fancy Bear, Lazarus Group oder Fancy Lazarus gingen und gehen in immer höherer Frequenz zielgerichtet an Unternehmen. Statt wahllos vorzugehen, variieren inzwischen die Lösegeldforderungen je nach Unternehmensgröße und Branche der Opfer. Tatsächlich waren während des gesamten Jahresverlaufs Unternehmen aus einer Vielzahl von Branchen (u.a. Finanzen, E-Commerce, Medien und Logistik) betroffen. Zwischen September und November wurden mehrere internationale VoIP-Anbieter angegriffen. Darunter auch die international agierenden Branchengrößen Bandwidth, VoIP.ms und Telnyx. Tagelang legten die Angriffe die Dienste der Service Provider lahm. Die Hacker-Gruppe REvil verantwortete einen Großteil der Angriffe und forderte Lösegelder in Höhe von bis zu 4,5 Millionen Dollar. [9]

Nach Angaben des US-Finanzministeriums und des Financial Crimes Enforcement Network (FinCEN) kann die Zahlung von Lösegeld in den USA sogar für illegal erklärt werden. Grund hierfür ist, dass die kriminellen Einnahmen Aktivitäten finanzieren könnten, die den nationalen Sicherheits- und außenpolitischen Zielen der Vereinigten Staaten zuwiderlaufen. Außerdem, so hieß es in der Erklärung, garantieren die Lösegeldzahlungen keinesfalls, dass gestohlene Daten wieder zurückkämen. Für US-amerikanische Unternehmen, die von Cyber-Erpressungen betroffen sind, ist die Situation doppelt bitter. [19]

Die Intensität und Aggressivität der Erpressungen ist nach Einschätzung der IT-Sicherheitsexperten von Link11 spürbar gestiegen. Das Ausmaß übertrifft die vielen cyberkriminellen DDoS-Aktivitäten, die bislang beim Schutz der zahlreichen Kunden in den vergangenen Jahren beobachtet wurden, bei Weitem. Mit jedem Tag melden sich weitere Unternehmen, die DDoS-Warn-Attacken nicht standhalten, schwerwiegende Ausfälle verzeichnen und über kurzfristige Notfallintegrationen Schutz suchen. Kostspielige Betriebsunterbrechungen, Produktionseinbußen, der Verlust von Daten und die langwierige Wiederherstellung der Systeme sind ansonsten mitunter die Folge.

Vorgehen der DDoS-Erpresser

Die Täter informieren sich im Vorfeld über die IT-Infrastruktur des Unternehmens und machen in der Erpresser-Mail eindeutige Angaben dazu, welche Server und IT-Elemente sie für die Warn-Attacken angreifen werden. Als Druckmittel starten die Angreifer teils mehrstündige Demo-Attacken, die sich durch hohe Volumen von bis zu 200 Gbps auszeichnen. Um diese Angriffsbandbreiten zu erreichen, denen im Allgemeinen nur dedizierte Schutzlösungen von spezialisierten Schutzanbietern standhalten, setzen die Täter Reflection-Amplification-Vektoren wie DNS ein. Sollten die Forderungen nicht erfüllt werden, drohen massive Hochvolumen-Attacken von bis zu 2 Tbps. Für den Transfer der Bitcoins an eine spezifische Bitcoin Wallet bleiben dem Unternehmen 7 Tage. Auch die EU-Strafverfolgungsbehörde Europol hat vermehrt beobachtet, dass Cyberkriminelle kleinere DDoS-Attacken starten und zeigen, welchen Schaden sie anrichten können, bevor sie mit größeren Angriffen drohen und Lösegeldforderungen stellen.

Die Beobachtung der Täter durch das LSOC hat gezeigt: Firmen, die einen professionellen und umfangreichen DDoS-Schutz nutzen, können ihre Ausfallrisiken deutlich reduzieren. Sobald die Angreifer merken, dass ihre Attacken ins Leere laufen, stoppen sie diese und ziehen sich zurück.

DDoS als Nebelkerze, um Datendiebstahl vorzubereiten

Kurz vor Weihnachten 2021 tauchten in einem Hackerforum 3,7 Millionen Kundendaten des US-amerikanischen Unternehmens FlexBooker auf. Eine Gruppe von Cyberkriminellen, die sich „Uawrongteam“ nennt, handelte mit den gestohlenen Daten, darunter E-Mail-Adressen, Namen, Telefonnummern und Passwort-Hashes sowie Kreditkartendaten im Dark Web. Berichten des digitalen Termin- und Kalenderdienstes FlexBooker zufolge ermöglichte ein massiver DDoS-Angriff auf den Amazon AWS-Server den Datendiebstahl. Erst nach der Aufarbeitung des DDoS-Angriffs gemeinsam mit Amazon stellte der digitale Kalenderdienst fest, dass mehr als drei Millionen Kundendaten gestohlen wurden. [20]

DDoS-Angriffe als Ablenkungsmanöver sind nicht neu. Gleichzeitig sind sie in der Regel kein immanenter Bestandteil eines solchen Datendiebstahls. Im Windschatten eines massiven DDoS-Angriffs können die Hacker jedoch unbemerkt durch die Hintertür in die Netzwerksicherheit eindringen und angreifen. DDoS-Angriffe verändern die Datenverkehrsprofile drastisch und erzeugen ein Rauschen, welches die Datenabschöpfung verschleiert, die das eigentliche Ziel dieser Angriffe ist. Die Intrusion Detection Systeme und Intrusion Prevention Systeme (IDS/IPS-Systeme), die zur Erkennung und Verhinderung von Datendiebstahl benötigt werden, reagieren extrem empfindlich auf DDoS-Angriffe. Da sie rechenintensive Überprüfungen jedes ein- und ausgehenden Pakets durchführen müssen, gehören sie zu den ersten Systemen, die von einem DDoS-Angriff überfordert werden.

> **Schützen Sie ihre Intrusion Detection Systeme und Intrusion Prevention Systeme (IDS/IPS-Systeme) am besten zusätzlich mit einem Cloud-basierten DDoS-Abwehrdienst.**
>
> **– Jag Bains,** Vice President Solution Engineering, Link11

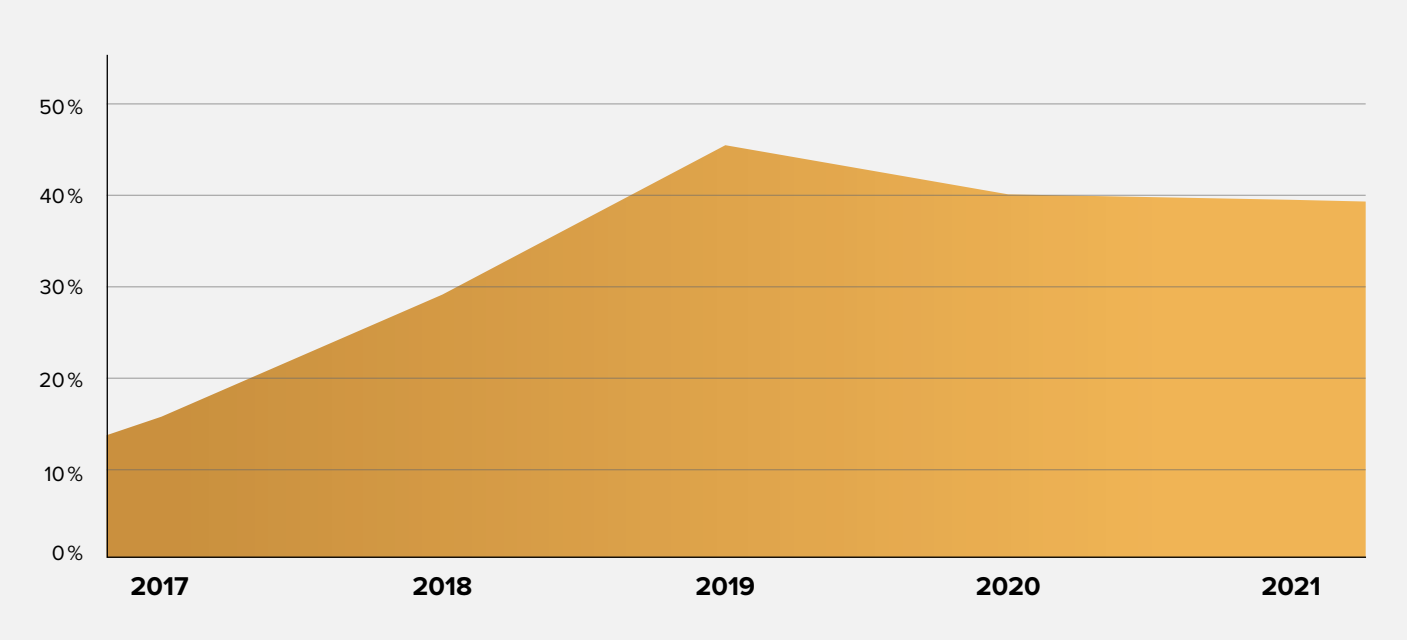
Zur Abwehr der DDoS-Attacke werden in kürzester Zeit die vorhandenen IT-Ressourcen mobilisiert, um die Systemausfälle und weitere Schäden zu minimieren. Das bedeutet, dass sich die IT-Verantwortlichen in erster Linie mit der Abwehr des Angriffs und der Wiederherstellung des Normalbetriebs beschäftigen. Da es bei DDoS-Angriffen auch zu längeren Ausfällen kommt, können die drohenden finanziellen Einbußen oder die Reputationsrisiken für Unternehmen beträchtlich sein.

Kommt es zu einer wie von FlexBooker geschilderten massiven DDoS-Attacke, werden sofort alle möglichen Abwehrmechanismen sowie Sicherheitsmaßnahmen eingeleitet. Die mit den DDoS-Angriffen verbundenen Ausfälle torpedieren den normalen Geschäftsablauf und erfordern eine rasche Lösung. Fehlt im Eifer des Gefechts der Blick auf das große Ganze oder wird die Möglichkeit eines vielschichtigen Angriffs ignoriert, kann der Schaden für das Unternehmen deutlich größer werden. Die Reichweite und Wirkung von DDoS-Angriffen sind in den vergangenen Jahren kontinuierlich gestiegen. Gerade Angriffe in denen DDoS als Nebelkerze genutzt wird, zeigen, dass die Gefahr immer größer wird. Umso wichtiger ist es, dass Unternehmen diese Sicherheitsrisiken ernst nehmen und einen strategischen Plan zur Erkennung und Abwehr von DDoS-Angriffen erstellen. Je schneller und präziser die DDoS-Attacken erkannt und abgewehrt werden, desto mehr Zeit gewinnen die IT-Mitarbeiter, um weitere Anomalien und Gefahren im Netzwerk aufzuspüren.

Cloud als etabliertes Angriffswerkzeug

Die Cloud-Nutzung im privaten und unternehmerischen Umfeld wächst stetig. Cloud-Provider bauen ihre Infrastrukturen entsprechend weiter aus. DDoS-Angriffe aus missbräuchlich dafür genutzten Cloud-Ressourcen, um entsprechende Bandbreiten und Rechenleistung zu generieren, haben sich inzwischen fest etabliert. Bei Analysen des LSOC zum Einsatz von Cloud-Servern bei DDoS-Attacken im Jahr 2017 lag der Anteil noch bei 16 %. In der Langzeitbetrachtung ist der Anteil, den missbrauchte Cloud-Server an DDoS-Traffic haben, kontinuierlich angestiegen und hat sich inzwischen auf einem Niveau von 40-45 % etabliert, mit Monatsspitzen bis zu 56 %. Das bedeutet, dass bei über jeder dritten bis zu jeder zweiten DDoS-Attacke im Jahr 2021 die Cloud als Angriffswerkzeug zum Einsatz kam. Dabei kompromittierten die Angreifer die Server-Instanzen öffentlicher Cloud-Service-Provider, indem sie sich über Schwachstellen oder Exploits Zugriff verschafften. Anschließend spielten sie ein vorgefertigtes Script auf, das den Server innerhalb von Minuten in einen DDoS-Bot verwandelt. Die Unternehmen, welche die Instanzen angemietet haben, bemerken diesen Fremdzugriff meist nicht oder erst sehr spät, wenn die Abrechnung kommt. Daneben erlangen Kriminelle über gestohlene Kreditkartendaten Zugang und mieten unter falschem Namen Cloud-Instanzen an. Für ihre Angriffe nutzen die Täter unterschiedlichste Anbieter von Public-Cloud-Services. Am häufigsten waren missbrauchte Server bei den drei internationalen Großanbietern Amazon Web Services (AWS), Google Cloud und Microsoft Azure registriert. Daneben nutzten die Angreifer auch Cloud-Angebote aus dem B2B-Bereich wie Oracle Cloud, DigitalOcean IBM Cloud.

Anteile Cloud Abuse



Was wir zukünftig vermehrt sehen werden

Carpet Bombing

Zu einer großen Herausforderung für Hosting- und Cloud-Anbieter können sich die sogenannten „Carpet Bombing"-Angriffe entwickeln. Diese Angriffe sind technisch komplex. Der Datenverkehr pro IP-Adresse ist so gering, dass viele Schutzlösungen sie nicht als Anomalie erkennen, was bedeutet, dass Angriffe oft unter dem Radar fliegen. Hinzu kommt, dass der Angreifer den DDoS-Verkehr nicht auf ein bestimmtes System oder einen Server lenkt. Es wird nicht nur eine IP-Adresse angegriffen, sondern ein ganzer Netzwerkblock mit mehreren hundert oder tausend Adressen. Unzureichend geschützt, ist es für Hosting- und Cloud-Provider fast unmöglich, das „Carpet Bombing" zu entschärfen.

Nach Einschätzung des LSOC hat diese Form des Angriffs eine neue Qualität erreicht.

Komplexe Attacken erfordern intelligente Lösungen

Die Angriffstechniken, die sowohl die Volumen- als auch die Netzwerk- und Applikationsebene attackieren, werden immer ausgefeilter. Komplexe und kombinierte Angriffsformen erschweren Unternehmen deren Abwehr. Schutzlösungen von der Stange, deren Patch- und Updatezyklen der Bedrohungslandschaft hinterherhinken, können nicht mithalten. Stattdessen sollten Unternehmen auf Systeme mit mehrschichtiger Anomalie-Erkennung und vernetzten Sicherheitsmechanismen setzen.

Präzision in der Erkennung und die Schnelligkeit in der Abwehr mittels intelligenter, adaptiver Systeme sind entscheidende Erfolgsfaktoren.

DDoS als Nebelkerze

Im Windschatten eines massiven DDoS-Angriffs können die Hacker unbemerkt durch die Hintertür in die Netzwerksicherheit eindringen und beispielsweise Malware platzieren, bevor sie die Webserver zum Durchbooten zwingen. Die vielfältigen Angriffsflächen, die unser digitales Leben, Arbeiten und Wirtschaften bietet, können in Zukunft noch besser ausgenutzt werden. Umso wichtiger ist es, dass Unternehmen diese Sicherheitsrisiken ernst nehmen und einen strategischen Plan zur Erkennung und Abwehr von DDoS-Angriffen erstellen.

Je schneller und präziser die DDoS-Attacken erkannt und abgewehrt werden, desto mehr Zeit gewinnen die IT-Mitarbeiter, um weitere Anomalien und Gefahren im Netzwerk aufzuspüren.

Erpressungen mit DDoS-Attacken werden zur Normalität

Für die kommenden Monate ist mit einem weiteren Anstieg von Lösegelderpressungen, wie sie seit dem Sommer 2020 in immer neuen und kürzer auftretenden Wellen zu beobachten sind, zu rechnen. Da Unternehmen ihre Digitalisierung weiter vorantreiben, bieten sie immer mehr Angriffsfläche und werden ohne unzureichenden Schutz anfälliger für Downtimes und Betriebsunterbrechungen.

Die geringen Kosten und die einfache Ausführbarkeit von DDoS-Angriffen werden dafür sorgen, dass Erpressungen weiterhin im Aufwind sind.

Quellen

1 https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

2 Telecompaper.com: Siminn reports DDoS attack hitting television service on 30 January, 03.02.2021

3 Lfpress.com: ‚Bot' attack slowed London area COVID-19 vaccine booking site: top doc, 22.03.2021

4 ORF.at: DDoS-Attacke: Österreichweite Ausfälle bei A1-Internet, 18.02.2021

5 Weirditaly.com: Lower House website under attack, 09.03.2021

6 Futurezone.at: Massive Cyberattacke legte Internet in Belgien weitgehend lahm, 06.05.2021

7 Illinoisnewstoday.com: Irish Internet Service Provider Hit by Cyber Attack, 17.08.2021

8 Securityaffairs.co: Major blackouts across Puerto Rico. Are the DDoS and the fire linked?, 14.06.2021

9 https://www.ispreview.co.uk/index.php/2021/09/ddos-attack-disrupts-voip-and-internet-services-at-voipfone-uk.html

10 https://www.bleepingcomputer.com/news/security/yandex-is-battling-the-largest-ddos-in-russian-internet-history/

11 https://www.newstalkzb.co.nz/news/business/cyber-attack-kiwibank-customers-still-having-access-issues/

12 https://www.inside-it.ch/de/post/heftiger-ddos-angriff-auf-berufsbildungszentrum-sdbb-20211008

13 https://taz.de/Hacker-Attacken-in-Spanien/!5813776/

14 https://www.rtlnieuws.nl/tech/artikel/5274188/ddos-aanval-gemeente-den-haag

15 https://de.statista.com/statistik/daten/studie/1189929/umfrage/anzahl-der-taeglich-aktiven-nutzer-von-microsoft-teams-welt-weit/

16 https://www.de-cix.net/de/unternehmen/medien/pressemitteilungen/datenverkehr-an-de-cix-internetknoten-macht-sprung-auf-ueber-38-exabyte

17 https://www.itpro.co.uk/security/cyber-crime/361523/europol-report-ddos-ransomware-gangs-evade-capture

18 https://www.cybertalk.org/2021/09/13/250000-strong-ddos-botnet-record-shattering-attacks/

19 https://www.gma-cpa.com/technology-blog/paying-ransom-on-a-ransomware-attack-is-illegal

20 https://www.cpomagazine.com/cyber-security/3-7-million-flexbooker-accounts-leaked-to-hacker-forum-after-ddos-attack/

Kontakt

Link11 GmbH
Lindleystr. 12
60314 Frankfurt

info@link11.com
+49 69 264929777