LINK11 INSIGHTS-FUNKTION

Mit hybriden DDoS-Schutzlösungen On-Prem-Investitionen optimieren

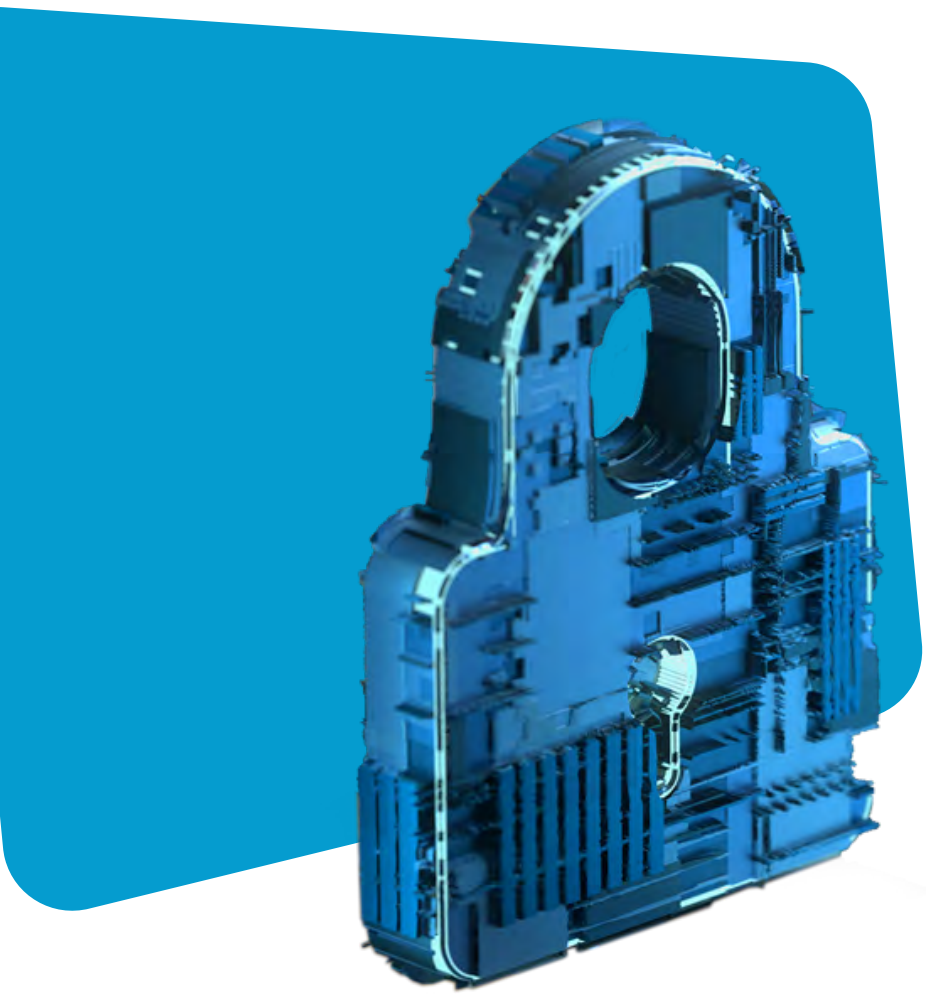
Whitepaper

Inhalt

Executive Summary

Unternehmen sind permanent durch Distributed-Denial-of-Service-Angriffe (DDoS) gefährdet, die immer gefährlicher werden[1]. Viele Unternehmen haben inzwischen bereits verschiedene Schritte unternommen, um sich gegen diese sich ständig weiterentwickelnde Bedrohung zu schützen. Am häufigsten kaufen Unternehmen eine On-Premise-Lösung, um sich vor DDoS-Angriffen zu schützen. Strategisch verbergen sich dahinter unterschiedliche Ansätze wie zum Beispiel der Kauf einer Firewall, einer hardware- oder softwarebasierten Schutzlösung. Allen gemeinsam ist, dass sie auf den unternehmenseigenen Servern oder vor Ort direkt implementiert sind. Obwohl der Kauf einer On-Premise-Lösung eine der häufigsten Strategien zur Abwehr von DDoS-Angriffen ist, stellen Unternehmen oft fest, dass diese Lösung nicht auf die Größe und Komplexität dieser Angriffe skaliert werden kann. Im Angriffsfall kann es dann zu Umsatzeinbußen, Reputationsschäden oder SEO-Verlusten und vielem mehr führen. Infolgedessen sinkt zudem die Unternehmensrendite auf Investitions- und Betriebskosten.

Um einen positiven Kosten-Nutzen-Effekt zu erzielen, haben sich hybride, cloudbasierte DDoS-Protection-Services durchgesetzt. Diese helfen einerseits den Unternehmen dabei, ihre Rendite zu maximieren und andererseits werden IT-Entscheider dabei unterstützt, ihre Investitionen vor Ort voll auszuschöpfen. Ergänzen Unternehmen ihre IT-Sicherheitsstrategie mit einem cloudbasierten DDoS-Schutz, kann dieser seine Schutzfähigkeiten voll entfalten. Große und komplexe Angriffe werden dynamisch entschärft, während die lokale Plattform kleine Angriffe bewältigen und Sicherheit auf der Anwendungsebene gewährleisten kann. Die einzelnen Cloud-DDoS-Protection-Anbieter bieten unterschiedliche Implementierungen und Funktionen eines solch hybriden Setups an. Trotz der verschiedenen Optionen bietet die Link11 Insights-Funktion mit ihren Kriterien eine Lösung für große, unkoordinierte sowie sehr spezialisierte und koordinierte DDoS-Angriffe, die mit den unterschiedlichsten Unternehmenskonfigurationen kombiniert werden kann.



On-Premise-Lösungen und ihre Einschränkungen

Immer mehr Geschäftsabläufe und Unternehmensprozesse werden online abgewickelt. Die Corona-Pandemie wirkte für diese Entwicklung wie ein Katalysator. Je mehr sich der Geschäftsalltag digitalisiert hat, desto größer ist der Bedarf für Sicherheitsmaßnahmen geworden. Besonders für den Schutz der wertvollen IT-Ressourcen haben Unternehmen verstärkt Sicherheitsmaßnahmen in der Regel in Form einer vor Ort installierten Edge-Defence eingeführt, wie z. B. eine Firewall. Diese Geräte wehren niedrigschwellige DDoS-Attacken auf einem niedrigen Level erfolgreich ab. Aus den folgenden Gründen versagen sie gleichzeitig bei mittelgroßen oder großen DDoS-Angriffen:

1. Die Kapazität dieser Geräte ist begrenzt. Edge-Geräte mit 10-Gbit-Ports sind, selbst wenn sie in der Lage wären, eine solche Leitungsrate zu bewältigen, mit der Größe aktueller DDoS-Angriffe leicht überfordert. Derartige Angriffe nehmen in Umfang und Dauer weiter zu.

2. Der Aktivitätsstatus (online oder Stand-by) dieser Geräte macht sie anfällig für State-Exhaustion-Angriffe. Ein kleiner, aber ausgeklügelter DDoS-Angriff kann leicht Zehntausende gleichzeitiger Verbindungen herstellen. Diese können die Statustabelle einer Firewall schnell überfordern und alle neuen gültigen Verbindungen blockieren.

3. Firewalls können einen grundlegenden Schutz vor DDoS-Angriffen bieten (z. B. Schutz vor SYN-, UDP- und ICMP-Floods). Dieser Schutz geht zu Lasten der Performance, was sich auf die erweiterten Funktionen der Firewall auswirkt (z. B. Layer-7-Inspektion, SSL-Entschlüsselung und VPN-Abschluss).

4. Mit Vor-Ort-Geräten sind vor allem Anwendungen und Systeme innerhalb des eigenen Rechenzentrums geschützt. Beim Schutz von Webanwendungen, die in öffentlichen Cloud-Infrastrukturen gehostet werden – ein wachsender Trend in Unternehmen – sind sie jedoch unwirksam.

> **Die Risikolandschaft wird immer unvorhersehbarer. Inzwischen sind die Angriffe sehr präzise und koordiniert, sodass die lokalen On-Premise-Lösungen oftmals überfordert sind.**
> **Gerade für diese sehr spezialisierten Angriffe zahlt sich eine cloudbasierte Schutzlösung aus.**
>
> **– Jag Bains,**
> Vice President Solution Engineering, Link11

Diese funktionalen Einschränkungen bei der Umsetzung einer On-Premise-Strategie können bei einem großen DDoS-Angriff zu einem Engpass führen oder sogar einen „Single Point of Failure“ darstellen. Dadurch wird der eigentliche Zweck dieser Lösung verfehlt – die wertvollen IT-Ressourcen zu schützen.

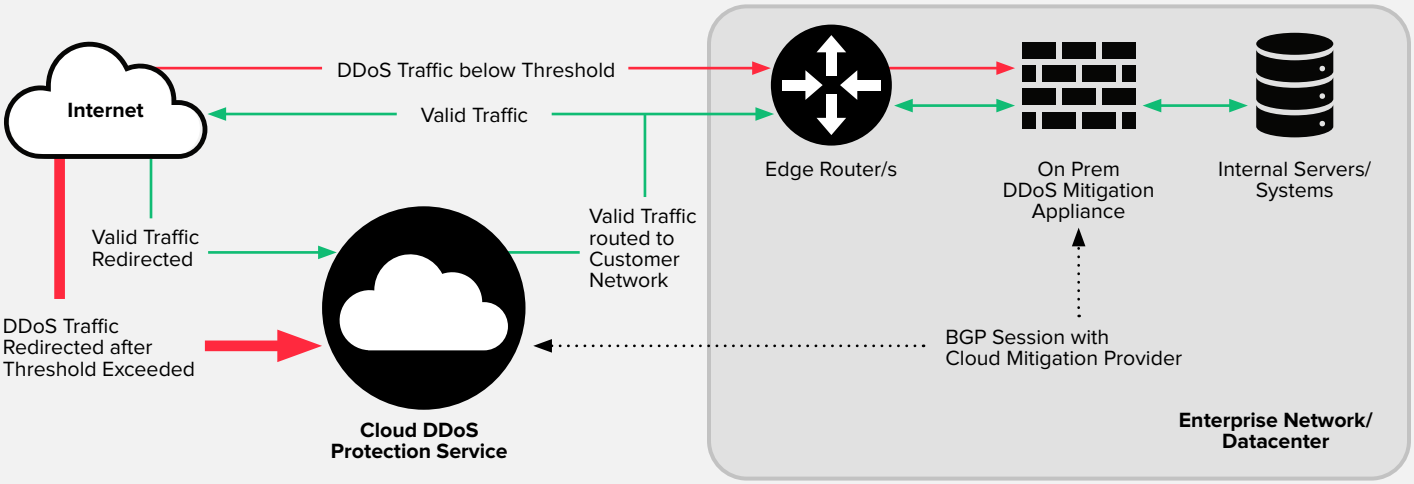
Die Hybrid-Lösung – das Beste aus zwei Welten

Eine hybride Lösung besteht darin, dass die Geräte vor Ort zusätzlich mit einem Cloud-DDoS-Schutz ausgestattet sind. Als cloudbasierte Schutzlösung kann diese Funktion große Mengen an volumetrischer sowie DDoS-Angriffe auf Protokoll- und Anwendungsebene absorbieren und den Datenverkehr filtern. Bösartiger Datenverkehr wird automatisiert und in Echtzeit herausgefiltert, sodass nur legitimer Datenverkehr das Unternehmen erreicht. Durch das Zusammenspiel einer lokalen und einer cloudbasierten Lösung können Unternehmen die Vorteile beider IT-Sicherheitsstrategien optimal nutzen. Dazu gehören einerseits die bereits getätigten Investitionen in die Vor-Ort-Installation und andererseits werden deren funktionalen Nachteile minimiert.

Der hybride Ansatz bedeutet, dass die vor Ort installierten DDoS-Schutz-Anwendungen die Angriffe lokal abschwächen, bis sie die Größe eines vorher festgelegten Schwellenwerts erreicht haben. Ist dieser erreicht, wird der Datenverkehr an die Cloud-DDoS-Schutzfunktion umgeleitet, in der Regel über das BGP-Protokoll. Der DDoS-Schutzanbieter sollte über eine Kapazität von mehr als einem Tbp/s zur Abwehr eines Angriffs verfügen. Damit sollten sämtliche Angriffsvektoren erkannt und blockiert und der legitime Datenverkehr zurück in das Kundennetz geführt werden. Sobald der Angriff unter den Schwellenwert auf ein bestimmtes Niveau sinkt, wird der Datenverkehr wieder direkt zurück in das Netzwerk des Unternehmens geleitet.

Ein solch hybrider Ansatz für den notwendigen DDoS-Schutz kombiniert die Stärken einer lokalen Schutzanwendung mit der Multi-Terabit-Skalierbarkeit der Cloud. Dadurch handelt es sich um eine sehr schnelle Lösung mit geringer Latenz für die meisten Angriffe, die bei Bedarf nahtlos weitere Kapazitäten bereitstellt.

Abbildung 1: Typische Hybrid-Topologie



Der Link11 Insights-Ansatz

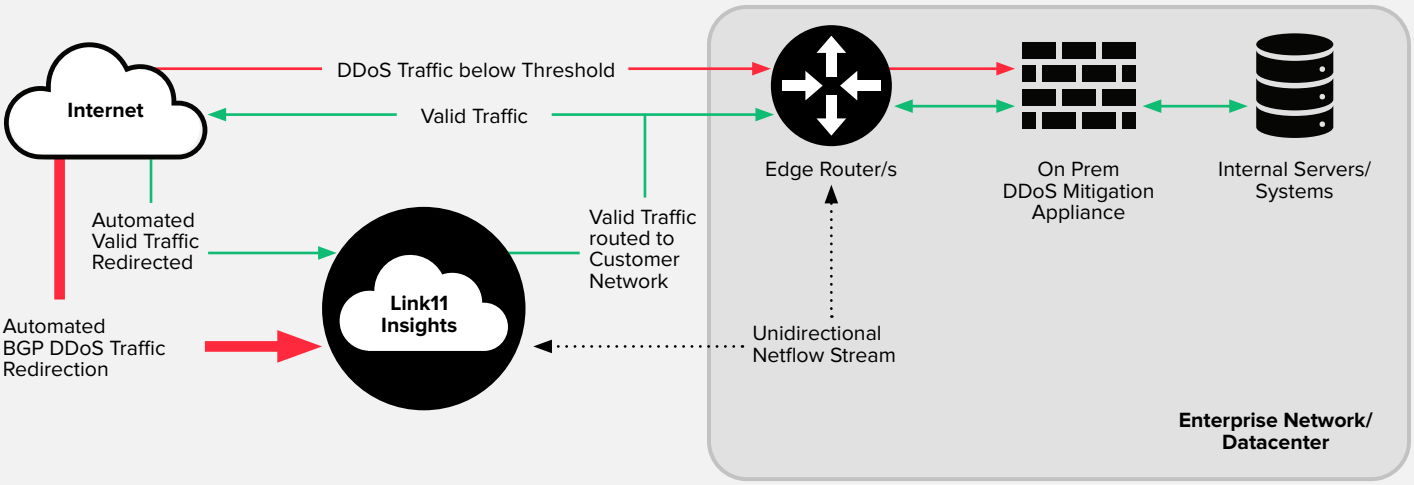
Ein typisches hybrides Setup hat viele hilfreiche Vorteile. Gleichzeitig erfordert ein solcher Aufbau oft eine Lösung eines einzigen Anbieters. Dieser kann veranlassen, dass der BGP-Datenverkehr des Unternehmens umgeleitet wird. Besonders für Unternehmen, die nicht über ein Security Operations Center rund um die Uhr verfügen, kann das sehr schwierig beziehungsweise kaum möglich in der Umsetzung sein.

Das hybride Link11 Produkt „Insights“ kontert diese Einschränkungen und bietet entscheidende Vorteile:

1. Technologieunabhängig: Die Link11 Insights-Funktion ist mit Hardware jeden Anbieters vor Ort kompatibel. Die Sicherheitslösung ist nicht auf bestimmte Hardware-Optionen beschränkt.

2. Mehrere Control-Plane-Optionen: Die meisten Hybrid-Lösungen benötigen eine BGP-Sitzung zwischen dem Kundennetzwerk und dem Cloud-Anbieter. Dies erfordert, dass der Kunde die Umleitung des Datenverkehrs zum Cloud-Anbieter initiiert, was oft ein manueller Vorgang ist. Mit der Link11 Insights-Funktion können Unternehmen weiterhin eine Standard-BGP-Sitzung verwenden und/oder einen Netflow-Export an die Insights-Funktion einrichten. Zudem wird die BGP-Umleitung automatisch vorgenommen, sobald ein Schwellenwert erreicht wird. Da Insights den eingehenden Netflow-Stream in Echtzeit analysiert, erkennt das System sofort, ob ein Schwellenwert erreicht wird. Daran schließt sich die automatische BGP-Umleitung an, ohne dass der Endkunde etwas tun muss (siehe Abb. 2).

Abbildung 2: Link11 Hybrid-Topologie



3. Mehrere Optionen für die Einstellung von Schwellenwerten. Die meisten hybriden Lösungen betrachten den gesamten Datenverkehrsdurchsatz innerhalb des Kundennetzwerks auf einer ausgewählten Gruppe von Schnittstellen, um festzustellen, ob eine Anomalie auftritt. Mit Insights können statt einer ausgewählten Gruppe viele Schwellenwert-/Bedingungsoptionen festgelegt werden, darunter:

- MB/s pro Sekunde,
- Pakete pro Sekunde,
- Anzahl der Traffic-Quelladressen,
- Anzahl der Quellländer,
- Anzahl der ISPs.

4. „Infrastruktur-Protection-Engine“: Das Herzstück der Link11 Insights-Funktion ist die „Infrastruktur-Protection-Engine“, die mehrere Strategien zur Abwehr und Abschwächung der DDoS-Angriffe einsetzt, darunter:

- Fingerprinting: Eingehender Datenverkehr wird analysiert und jedem Client wird ein eindeutiger „Fingerabdruck“ zugewiesen. Jeder Fingerabdruck umfasst Hunderte von einzigartigen Eigenschaften und ist weitaus differenzierter als eine IP-Adresse. Auf diese Weise wird sichergestellt, dass legitime Benutzer auf Ressourcen zugreifen können, während Fingerabdrücke, die bekannte Angriffsmuster enthalten, blockiert werden.
- KI-Analyse: Das selbstlernende KI-Modul der Funktion analysiert den Datenverkehr auf bösartige Aktivitäten und kann sogar vor KI-gesteuerten Angriffen warnen. Das Modul unterbricht aktiv Angriffe, indem es falsche Informationen an Angreifer sendet. Dem Angreifer wird suggeriert, dass ein Asset „abgeschaltet“ wurde, obwohl es für legitime Nutzer zugänglich bleibt.
- Gegenproben des Datenverkehrs anhand von Bedrohungsdaten: Die Funktion gleicht den gesamten Datenverkehr mit Echtzeit-Bedrohungsdaten ab. So wird festgestellt, ob der Datenverkehr bekannten bösartigen Aktivitäten entspricht. Dadurch kann die Funktion bösartige Aktivitäten blockieren, während sie legitime Anfragen akzeptiert.

Jedes Mal, wenn die Funktion eine neue Bedrohung identifiziert, wird die Angriffssequenz in einer Datenbank gespeichert, um sie später wieder aufrufen zu können. Erkennt das Modul dieselbe Angriffssequenz erneut, wird sie sofort blockiert.

Das Ergebnis dieser kombinierten Strategien: Die kürzeste Zeit bis zur Schadensbegrenzung im Vergleich zu führenden internationalen Sicherheitsanbietern, wie eine unabhängige **Studie von Frost & Sullivan** zeigt[2]. Abbildung 3 zeigt die Time-to-Mitigate (TTM) zwischen Link11 und anderen führenden Anbietern von cloudbasierten Schutzlösungen:

Abbildung 3: Vergleichsübersicht Time-to-Mitigate

	Link11	Arbor Cloud/ Neustar	Cloudflare Magic Transit	Imperva Incapsula	Akamai Prolexic
UDP bandwidth flood	21 secs.	4 mins.	fail	1 mins.	up to 59 secs.
UDP DNS refl/amp bandwidth flood	18 secs.	4 mins.	4 mins.	1 mins.	up to 59 secs.
Fragmented IP bandwidth flood	0 secs.	4 mins.	4 mins.	2 mins.	up to 59 secs.
TCP SYN flood	0 secs.	4 mins.	2 mins.	1 mins.	5 mins.
TCP SYN-ACK flood	12 secs.	4 mins.	up to 59 secs.	2 mins.	8 mins.
TCP RST „carped bomb“	1 min 20 secs.	fail	fail	1 mins.	5 mins.
HTTPS GET request flood-404	18 secs.	4 mins.	fail	fail	fail
Average TTM	21 secs.	240 secs.	150 secs.	80 secs.	180 secs.

Optionen und Überlegungen für Tech-Führungskräfte

Je nachdem, wie viel Unternehmen in ihre On-Premise-Strategie investiert haben und in welchem Stadium des Hardware-Lebenszyklus sich diese befindet, sind die Herausforderungen und die dafür notwendigen Überlegungen unterschiedlich. Hat das Unternehmen eine neue Implementierung, ist der IT-Entscheidungsträger angehalten, seine Investition maximieren. Eine Anbindung an die Link11 Insights-Funktion wird dies gewährleisten.

Läuft der Vertrag in Kürze aus und muss erneuert werden, sollte der CISO seine Planung überdenken und eine reine Cloud-Lösung mit Insights in Betracht ziehen. Mit Insights erhalten Unternehmen eine enorme Kapazität und die Fähigkeit, volumetrische und protokollbasierte Angriffe sowie komplexe Angriffsvektoren mit der fortschrittlichen „Infrastruktur Protection Engine“ zu vereiteln.

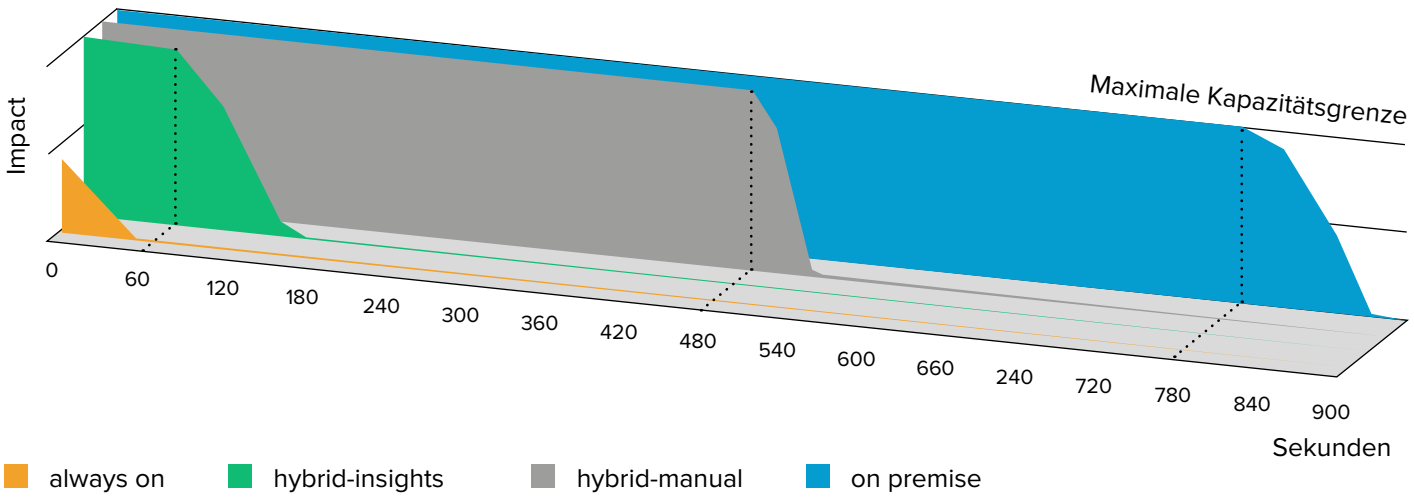
Darüber hinaus sollte der CISO den Always-On-Modus in Betracht ziehen, wenn die Toleranz des Unternehmens für Ausfallzeiten sehr gering ist. Im Always-On-Modus wird der Datenverkehr des Kunden immer durch die Link11-Cloud geleitet, wo er überprüft, gefiltert und bösartiger Datenverkehr abgewehrt wird. Zudem entfällt in diesem Modus die Zeit für die Aktualisierung der globalen BGP-Routentabelle, die zwischen 45 und 90 Sekunden dauern kann[3]. Mit der kurzen Time-to-Mitigate (TTM) von Link11 werden die Ausfallzeiten minimiert, was die Kosten und die betriebliche Belastung innerhalb des Unternehmens reduziert.

> **Je schneller und präziser DDoS-Angriffe mitigiert werden, desto größer wird der positive Kosten-Nutzen-Effekt der Insights-Funktion für Unternehmen sein.**
>
> **– Marc Wilczek,**
> Geschäftsführer, Link11

Die folgende Grafik soll die Bedeutung der TTM veranschaulichen. Die Grafik zeigt die TTM bei der Entschärfung eines 15-minütigen, mittelgroßen Angriffs (z. B. 20 GB/s), der die Kapazität eines Unternehmensnetzwerks auslasten kann. Daneben wird die TTM in vier verschiedenen Modi verglichen:

a) Always On. In diesem Modus läuft der Datenverkehr immer über die Link11 Cloud-DDoS-Plattform.
b) Hybrid Insights. Hier nimmt Link11 automatisch die BGP-Umleitung vor.
c) Hybrid Manual. Hier muss das Unternehmen selbst die notwendigen BGP-Änderungen vornehmen, um den Datenverkehr zum Cloud-DDoS-Schutzanbieter umzuleiten.
d) On-Premise. Das Unternehmen nutzt ausschließlich seine On-Premise-Lösung.

Impact by Solution



Die oberste Linie auf der y-Achse stellt die maximale Kapazitätsgrenze des Datenverkehrs bzw. Bandbreiten dar. Wird diese erreicht, kommt es zu einem Ausfall und potenziellen Kollateralschäden im Unternehmensnetz. Deutlich ist, dass die TTM stark zwischen den verschiedenen Modi variiert:

a) Always on: Die maximale Kapazitätsgrenze wird nie erreicht und die Entschärfung erfolgt innerhalb von Sekunden.
b) Hybrid Insights: Die automatische BGP-Umleitung kann immer noch 45–60 Sekunden dauern, bis die globalen Routentabellen konvergieren. Bis der Datenverkehr vollständig zur Link11-Funktion umgeleitet ist, tritt eine vorübergehende Blockade ein.
c) Hybrid Manual: Es kann noch rund 7 Minuten dauern, um die Ziel-IP zu identifizieren und die notwendigen BGP-Änderungen für das Unternehmen vorzunehmen. Die Dauer kann noch länger sein, wenn das Unternehmensnetzwerk kein IT-Netzwerk-Operationcenter rund um die Uhr betreibt und auf Bereitschaftspersonal zurückgreifen muss.
d) Vor-Ort-Lösungen: Lokale Geräte wären einem Angriff über die gesamte Dauer komplett ausgeliefert. Bis der Carrier über den Angriff in Kenntnis gesetzt wurde und das sogenannte „Blackholing“ bei den verschiedenen Upstream-Anbietern implementiert hat, sind sämtliche Dienste und Anwendungen nicht verfügbar.

Zu den Kosten eines durch einen DDoS-Angriff verursachten Ausfalls gehören Umsatzeinbußen, die Wiederherstellung von Diensten und zusätzliche betriebliche Allgemeinkosten. Diese Einbußen wurden auf durchschnittlich 5.600 USD pro Minute Ausfallzeit geschätzt[4]. Auf Basis dieser Schätzungen würde eine reine Vor-Ort-Strategie bei dem angenommenen 15-minütigen DDoS-Angriff Kosten in Höhe von 84.000 US-Dollar verursachen. DDoS-Angriffe werden immer größer, nachhaltiger und komplexer. Diese Kosten werden im Fall eines Angriffes und der damit verbundenen Downtime ohne eine angemessene und effiziente Lösung weiter steigen.

Wenn Sie mehr wissen möchten, dann sprechen Sie mit den Cyber-Resilienz-Experten von Link11. Für einen ganzheitlichen Schutz von IT-Infrastrukturen und kritischen Anwendungen und zur Stärkung der Cyber-Resilienz setzt Link11 mit seiner Insights-Funktion auf künstliche Intelligenz, maschinelles Lernen, Automatisierung und Echtzeit-Abwehr. Wir freuen uns, Sie zu dem Thema zu beraten und Alternativen aufzuzeigen.

Ihr Ansprechpartner für hybride Schutzlösungen und deren Vorteile:

Jag Bains
Link11 GmbH,
Vice President Solution Engineering
j.bains@link11.com

Quellen

1 https://www.link11.com/de/downloads/ddos-report-h1-2022

2 https://www.darkreading.com/vulnerabilities-threats/link11-sets-new-standards-in-ddos-protection-as-test-winner

3 https://www2.cs.arizona.edu/~bzhang/paper/04-globecom-destreach.pdf

4 https://bigdata-madesimple.com/ddos-attacks-on-the-rise-a-closer-look-at-the-data

LINK11

www.link11.com

www.linkedin.com/company/link11/

twitter.com/link11gmbh

info@link11.com

Kontakt

Link11 GmbH
Lindleystr. 12
60314 Frankfurt