LINK11

DDoS Protection Buyer’s Guide

Die richtige Schutzlösung gegen Distributed Denial of Service-Attacken für Ihr Unternehmen

DDoS Protection Buyer's Guide

Die richtige Schutzlösung gegen Distributed Denial of Service-Attacken für Ihr Unternehmen

DDoS-Service- und Lösungsprovider unterscheiden sich teilweise erheblich in ihrem Leistungsumfang. Die Entscheidung für eine Schutzlösung fällt daher oft nicht leicht. In diesem Buyer's Guide erfahren Sie, worauf Sie bei der Auswahl einer DDoS-Schutzlösung achten sollten und wie Ihr Unternehmen von der Zusammenarbeit mit einem externen Schutzanbieterprofitieren kann. Sie erhalten Informationen über grundlegende Funktionen moderner DDoS-Schutzlösungen, die Sie bei den Anbietern gezielt abfragen sollten.

Inhalt

Lösungsansätze beim DDoS-Schutz 3
- CDN 3
- Hardware Appliances 3
- Cloudbasierter DDoS-Schutz 4
- Cloudnativer Ansatz (AWS/Azure) 4
- Hybrid Schutz 5

Integration von DDoS-Schutzlösungen 5
- DDoS-Schutz via DNS Forwarding 5
- DDoS-Schutz via Border Gateway Protocol (BGP 6
- Kombinationsmöglichkeiten: Web DDoS und Infrastrukturschutz 6

Verfügbarkeit: always-on oder on-demand 6
- On-demand-Schutz 6
- Always-on-Schutz 6

Filtermöglichkeiten 7

Automatisierung in Angriffserkennung und -filterung 7

Schutz für OSI-Layer 8

Service Level Agreements 8
- SLA auf die Schutzbandbreite 8
- SLA bei Time to Mitigate 9
- SLA bei Service Uptime 9

Skalierbarkeit der Gesamtlösung 10

Multicloud Support 10

Compliance 10

Dashboard mit Konfigurationsmöglichkeiten 11

Preisgestaltung und Kosten 11

Integrierte Plattform für DDoS-nahe Dienste 12

Support 12

Fazit 13

Über Link11 13

Checkliste 14

Lösungsansätze beim DDoS-Schutz

Beim Schutz vor DDoS-Attacken stehen mehrere Varianten zur Auswahl: CDN, Hardware Appliances, cloudbasierter sowie cloudnativer DDoS-Schutz und hybride Schutzlösungen.

CDN

Das Content Delivery Network (CDN) verteilt Inhalte der Webseite auf weltweit platzierte Server. Somit müssen Anfragen nicht vom Original-Server beantwortet werden. Das hilft, Lastspitzen, wie sie durch großvolumige DDoS-Attacken entstehen können, bis zu einem gewissen Level auszugleichen.

- ⊕ Schutz vor Volumenangriffen
- ⊖ Schutzniveau entspricht maximaler Außenanbindung
- ⊖ Nicht alle Angriffsarten abgedeckt
- ⊖ Viele der Anbieter stammen aus den USA und sind damit u.a. dem Patriot Act unterworfen. Das heißt, sie müssen Daten auf Verlangen von US-Behörden herausgeben. Der Compliance-Aspekt wird durch das Aus für den EU-US Privacy Shield durch den Europäischen Gerichtshof im Juli 2020 weiter verschärft (siehe dazu Kapitel „Compliance“).

Hardware Appliances

Es wird ein Gerät (DDoS-Appliance) in der Infrastruktur des Unternehmens oder im Backbone des Providers installiert. Diese Appliance überwacht den Datenverkehr. Bei Auffälligkeiten wie dem plötzlichen Anstieg des Datenverkehrs limitiert sie den Traffic bzw. erkennt die Anfragen des Angreifers und blockiert diese. Bei einigen Deployment-Modellen sind manuelle Eingriffe notwendig - entweder durch die unternehmenseigene IT-Abteilung oder einen externen Sicherheitsdienstleister. Dies erfordert Zeit und physische Präsenz, die in Zeiten von Home-Office und Remote-Work nicht immer gewährleistet werden kann.

- ⊕ Individuelle Anpassungen an kundenspezifische IT-Infrastruktur und Datenverkehr
- ⊖ Gegen Attacken, die über die verfügbare Internetbandbreite hinausgehen, können sie keinen Schutz bieten (Schutzniveau entspricht maximaler Außenanbindung)
- ⊖ Kein Machine Learning zur Erkennung neuer Angriffsvektoren möglich, siehe Kapitel „Automatisierung in Angriffserkennung und -filterung“
- ⊖ Insellösung ohne Berücksichtigung hybrider IT-Infrastrukturen mit einem oder mehreren Cloud-Diensten
- ⊖ Hohe Anschaffungskosten (Capex) sowie eigene Betriebskosten samt Personalaufwände (Opex)
- ⊖ Aufwändige Integration in bestehende IT-Infrastruktur
- ⊖ Viele der Anbieter sind US-Anbieter und damit u. a. dem Patriot Act unterworfen, das heißt, sie müssen Daten auf Verlangen von US-Behörden herausgeben, siehe Kapitel „Compliance“

Cloudbasierter DDoS-Schutz

Der Datenverkehr einer Webseite wird über den externen Filter des DDoS-Schutzanbieters geleitet. Durch eine mehrstufige Analyse der Anfragen können Angreifer erkannt und blockiert werden. Nur legitimer Datenverkehr wird weitergeleitet.

- ⊕ Gute Angriffserkennung von Volumen-, Applikations- und Protokollattacken sowie von noch unbekannten Angriffsvektoren
- ⊕ Hohe Bandbreitenstärke
- ⊕ Faktisch unbegrenzte Skalierbarkeit
- ⊕ Schnelle und einfache Integration
- ⊕ Ganzheitlicher Schutz komplexer IT-Landschaften samt den lokalen, globalen und cloudbasierten Infrastrukturen des Unternehmens
- ⊕ Redundanz
- ⊖ Datenschutzstandards des Landes sind zu beachten
- ⊖ Betrieb durch Drittanbieter

Cloudnativer Ansatz (AWS/Azure)

Für eine schnelle Implementierung werden cloudnative DDoS-Schutzlösungen mit einem Basis-Set an Optionen und Security-Einstellungen ausgeliefert. Diese eignen sich für DevOps-Projekte. In der Praxis reichen diese aber häufig nicht aus, um die Integrität der Applikationen und Daten im Rahmen von Produktivumgebungen sicherzustellen. Da der Nutzer gegenüber Dritten in der Pflicht für die Sicherheit und den Datenschutz steht, sind umfangreiche Anpassungsarbeiten und tiefgehende Kenntnisse in Security notwendig.

Sicherheitsfeatures als Bestandteil von Cloud-Computing-Lösungen sind nicht konzipiert, um gezielte Angriffe oder Mega-Attacken abzuwehren. Vielfach kommen die Angriffe aus derselben Cloud-Umgebung. Eine transparente Auskunft zum Schutzlevel oder zu Möglichkeiten individueller Sicherheitseinstellungen bieten die meisten Cloud-Provider jedoch nicht.

- ⊕ Angriffserkennung von Volumen-, Applikations- und Protokollattacken sowie von noch unbekannten Angriffsvektoren
- ⊕ Hohe Bandbreitenstärke
- ⊕ Skalierbarkeit
- ⊖ Insellösung, die nur plattformspezifisch alarmiert, schützt und reportet, Administrationsaufwand bei Multicloud-Szenarien daher sehr hoch, siehe Kapitel „Multicloud-Support“
- ⊖ Bisweilen ist der Schutz nur für ausgewählte Dienste beim Public-Cloud-Anbieter verfügbar, nicht aber vollumfänglich für alle dort betriebenen Services
- ⊖ Unklarheit beim Schutz, wenn Angriffe auf die Cloud-IT eines Unternehmens aus derselben Cloud-Umgebung stammen
- ⊖ Alarming Auditing zum Teil nur gegen Aufpreis möglich

- Cloud-Anbieter bieten Basis-Schutz. Advanced Protection kostspielig
- Keine oder Basis-SLAs, die bis zu 20 Minuten Reaktionszeit vorsehen
- Fehlende Transparenz zur Funktionsweise des Schutzes (Design Authority)
- Eingeschränktes Logging und Reporting
- Keine Individualbetreuung
- Datenschutzstandards des Landes sind zu beachten

Hybrid Schutz

Die Kombination aus Hardware- und Cloud-Schutzlösung bietet einen umfangreichen integrierten Schutz gegen kombinierte Angriffe auf Anwendungs- und Netzwerkebene.

- Doppelte Absicherung
- Schutz der gesamten Infrastruktur
- Hohe Bandbreitenstärke, die bei der Hardware-Lösung jedoch stark limitiert ist
- Hohe Anschaffungskosten für die Appliance sowie laufende eigene Betriebskosten samt Personalaufwände
- Aufwändige Integration in bestehende IT-Infrastruktur
- Unzureichender Schutz für Public-Cloud-Dienste
- Geringe Automation
- Latenz und Ausfallzeiten im Angriffsfall durch Schwenkvorgang
- Datenschutzstandards des Landes sind zu beachten

Integration von DDoS-Schutzlösungen

DDoS-Schutz kann über ein Weiterleiten per DNS Forwarding implementiert werden, oder der Datenverkehr wird im Angriffsfall per BGP zum Schutzanbieter bzw. seine Scrubbing Center geleitet und gefiltert. Der Aufbau der IT-Systeme im Unternehmen ist für die Wahl zwischen den beiden Integrations-Varianten entscheidend.

DDoS-Schutz via DNS Forwarding

Die Integration der Schutzlösung via DNS zielt auf die Absicherung von Webanwendungen eines Unternehmens. Eine Aufstockung der Serverinfrastruktur, zusätzliche Bandbreite oder neue Router-Technologie sind nicht notwendig. Die Integration via DNS lässt sich bereits ab einer IP-Adresse umsetzen und schützt Anwendungen, die auf Domainnamen basieren, vor DDoS-Attacken auf Layer 3-7. Hierfür werden die DNS A-Record-Einträge der betroffenen Anwendung angepasst, wodurch der Datentransfer in das Scrubbing Center umgeleitet wird. Die Clients fragen die DNS-Server nach der IP-Adresse, erhalten durch die DNS-Umstellung die IP-Adresse des Scrubbing Centers und sendet die Attacke daher nicht an den Originalserver. Der Schutz über DNS Forwarding ist sofort aktiv, nachdem die Umstellung im DNS-Server erfolgt ist.

DDoS-Schutz via Border Gateway Protocol (BGP

Die BGP-Variante bietet einen umfassenden Schutz des gesamten Unternehmensnetzwerks und schützt dadurch auch alle elementaren Unternehmensanwendungen wie Mail, VPN, Webserver etc.

Der BGP-DDoS-Schutz kann in einer On-demand-Variante eingesetzt werden und behält den normalen Datenfluss bei, solange kein Angriff stattfindet. Nur im Angriffsfall wird der Datentransfer über das Scrubbing Center geleitet. Die gefilterten Datenpakete werden über einen geschützten Tunnel (VPN, IPsec, GRE) an das Kundennetzwerk zurückübertragen. Nachdem die DDoS-Attacke erfolgreich abgewehrt wurde, wird der Datentransfer wieder über die ursprüngliche Route geleitet.

Der Einsatz der BGP-Lösung setzt für das Umrouting ein /24 oder größeres IP-Netz voraus. Sowohl der Kunde als auch das Security Operations Center können bei einer Standby-Integration im Angriffsfall das Netz announcen.

Durch die Erweiterung mit einem Monitoring, das kundenseitig auf Flow-Daten lokaler Router basiert, kann im Angriffsfall der DDoS-Schutz automatisch und ohne manuelle Interaktion aktiviert werden.

Daneben ist der BGP-DDoS-Schutz auch im Always-on-Betrieb verfügbar. Für Details zur permanenten oder temporären Schutzinstallation siehe Kapitel „Verfügbarkeit: always-on oder on-Demand“.

Kombinationsmöglichkeiten: Web DDoS und Infrastrukturschutz

Die IT-Infrastruktur von Unternehmen wird immer komplexer und umfasst zunehmend verschiedene IT-Systeme: vom Webserver über Datenbanken und Internettelefonie bis zu Cloud-Anwendungen. Für ein Höchstmaß an DDoS-Schutz auf Layer 3 bis einschließlich Layer 7 ist die Kombination von DNS Forwarding und BGP-Umleitung empfehlenswert. Die Entscheidung darüber sollte immer unternehmensspezifisch getroffen werden und auf Basis einer gründlichen Analyse in Zusammenarbeit mit dem zu beauftragenden DDoS-Schutzanbieter erfolgen.

Verfügbarkeit: always-on oder on-demand

Unternehmen haben die Wahl, ob die externe Schutzlösung permanent (always-on) den Datenstrom filtern soll oder nur im Angriffsfall (on-demand).

On-demand-Schutz

Beim On-demand-Schutz fließt der Datenverkehr in gewohnter Weise zum Unternehmen, unterliegt aber einem ständigen Monitoring (zumeist basierend auf Flow-Daten). Im Falle eines Angriffs wird das Unternehmen automatisch informiert und der Verkehr auf das Scrubbing Center umgeleitet und gefiltert. Der nun bereinigte Datenverkehr fließt vom Scrubbing Center über den schon vorbereiteten Direct Connect oder GRE-Tunnel zum Unternehmen weiter. Durch den Netzwerkschwenk greift der Schutz mit einigen wenigen Minuten Verzögerung. Ist der Angriff vorbei, wird das Netz zurückgeschwenkt. Schießt sich ein Angreifer auf das Unternehmen ein und greift es über einen längeren Zeitraum wiederholt an, muss das Netzwerk jedes Mal neu announct werden.

Always-on-Schutz

Ein erhöhter dauerhafter Schutzbedarf kann auch durch eine intensivere Nutzung bestimmter Unternehmensdienste wie VPN-Zugänge im Rahmen von Home-Office- und Remote-Work-Strategien entstehen. Die Alternative zum On-demand-Schutz besteht in der Installation eines dauerhaften Schutzes. Beim Always-on-Schutz – sowohl via DNS Forwarding als auch in der BGP-Umleitung – wird der Datenverkehr permanent über ein Scrubbing Center geleitet. Dieser Ansatz stellt 365 Tage im Jahr, 24/7 eine zuverlässige Absicherung der Unternehmens-IT sicher. Gleichzeitig sorgen die dauerhafte Filterung und die Bereinigung des Datenverkehrs für eine Entlastung der unternehmenseigenen IT-Infrastruktur.

Andererseits sollten DDoS-Schutzanbieter flexible Deployment-Modelle anbieten. Die Kombination von Always-on- und On-demand-Lösungen hilft dabei, die unterschiedlichen Schutzbedürfnisse zunehmend komplexer Infrastrukturen zu adressieren. Beispielsweise können Unternehmen für ihre Applikationen den Always-on-Schutz wählen und ihn mit einem eventgetriebenen On-demand-Schutz für E-Mail- und Webserver kombinieren.

Filtermöglichkeiten

Grundsätzlich existieren zwei verschiedene Methoden für die die Filterung des Datenverkehrs: die Filterung nach statischen und die Filterung nach dynamischen Heuristiken.

Statische Analyse
Statische Filter greifen bei der Überprüfung des Datenverkehrs auf vordefinierte Regeln zurück (Blacklist). Die Blacklist umfasst Filterregeln für bekannte Angriffsformen. Treten beim Abgleich der Verhaltensmuster bestimmter Anfragen Übereinstimmungen mit Heuristiken der Blacklist auf, wird der Traffic als DDoS klassifiziert.
Typische statische Filterregeln sind:

- Protokoll (TCP, UDP, ICMP etc.)
- TCP-Flags, ICMP-Typ
- Quell- und Ziel-IP
- Rate-Limit pro IP bzw. Netzbereich

Eine Filterung des DDoS-Traffics nach statischen Regeln ist nur so gut wie die hinterlegte Blacklist. Enthält sie für bestimmte oder neue Angriffe kein zugeschnittenes verhaltensbasiertes Muster, kann der Angriff als solcher nicht erkannt werden.

Dynamische Analyse
DDoS-Angreifer identifizieren permanent neue Schwachstellen und offene Services, die sich für Überlastungsangriffe missbrauchen lassen. Zuletzt zeigten Memcached- und CLDAP-Attacken, aber auch das Aufkommen der Vektoren WS-Discovery, Apple Remote Control und DVR DHCPDiscovery, dass Unternehmen ständig mit neuen Angriffstechniken rechnen müssen.
Filtermethoden, die proaktiv nach auffälligen, aber noch nicht definierten Verhaltensmustern suchen, gehört daher die Zukunft. In Friedenszeiten lernt die Schutzlösung im ersten Schritt das legitime Traffic-Profil einer Webseite oder eines Netzwerkes und leitet daraus Normbereiche ab (Whitelist). Abweichungen und ungewöhnliche Verhaltensmuster werden automatisch durch den Einsatz von Maschinellem Lernen und Künstlicher Intelligenz (KI) erkannt (siehe auch Kapitel „Automatisierung in Angriffserkennung und -filterung“), noch bevor es überhaupt zum Schaden kommt. Diese dynamischen Muster werden wiederum als neue Filterregeln hinterlegt.

Automatisierung in Angriffserkennung und -filterung

Menschliches Versagen ist der häufigste Grund für Sicherheitsprobleme. Aufgrund der steigenden Anzahl von Alarm-Meldungen können wichtige Ereignisse schnell untergehen. Um eine Echtzeitreaktion und hundertprozentige Angriffserkennung für sowohl bekannte als auch neue, noch unbekannte Attacken-Formen zu gewährleisten, müssen Prozesse für schnelle und zuverlässige Analysen voll automatisiert werden und auf Künstlicher Intelligenz basieren.
Im Idealfall verwendet die DDoS-Schutzlösung „lernende“ Filterprozesse, die zuvor anhand legitimer Besucher der Webseite gründlich eingemessen wurden. DDoS-Schutz basiert dann nicht auf simplen und statischen Ausschlussmethoden, sondern auf ausgeklügelten, statistischen Verhaltensmodellen, die vom Normalverhalten abweichende IPs sofort erkennen und aussperren. Dadurch ist eine sehr geringe sogenannte „False-Positive-Rate“ gewährleistet. Während in der Vergangenheit beim DDoS-Schutz vor allem ein Blacklisting-Ansatz gewählt wurde, setzt sich immer mehr das Whitelisting durch, das im Sinne einer Beweislastumkehr funktioniert. Das bedeutet: Alles, was nicht dem legitimen Datenmuster entspricht (Whitelisting), ist auffällig und potenziell bedrohlich.

Workflow bei manueller Abwehr von DDoS-Attacken	Workflow bei automatisierter Abwehr von DDoS-Attacken
Ein Sicherheitsvorfall wird erkannt und gemeldet, z. B. durch eine E-Mail an das SOC	Der Vorfall wird automatisch erkannt
Das SOC leitet die Reaktion auf den Vorfall ein	Die Mitigation wird aktiviert
Validierung durch das SOC ist abgeschlossen und der Schutz aktiviert	Das System hat aus diesem Angriff bereits für den nächsten Angriff gelernt

DDoS-Schutzlösungen sollten den eingehenden Traffic granular untersuchten und jeden Client mit einem digitalen Fingerabdruck versehen. Diese Unterscheidung ist viel differenzierter als eine Identifizierung per IP-Adresse. Sie macht es außerdem möglich, dass reguläre Besucher auch im Angriffsfall auf die betroffenen Systeme zugreifen können, ohne den Filterungsprozess überhaupt zu bemerken. Wenn im Fingerabdruck bereits bekannte Angriffsmerkmale identifiziert werden, wird der Client bei der ersten Anfrage geblockt.

Als nachgelagerter Schritt sollte der eingehende Traffic unter Einsatz von Maschinellem Lernen und Künstlicher Intelligenz analysiert und mit historischen Daten zu bereits bekannten Angriffsmustern abgeglichen werden. Wenn die Schutzlösung einen Angriff erkennt, wird gezielt nur dieser DDoS-Traffic in einem der weltweiten Filter-Cluster geblockt, während der legitime Datenverkehr passieren darf. Anders als bei einer Schutzlösung, die auf die Verteilung von Content ausgerichtet ist, wird die Last jedoch vollständig aus dem Traffic entfernt. Auf diese Art und Weise läuft der gesamte Filterprozess im Hintergrund ab und bleibt vor den Usern verborgen. Für eine kontinuierliche Verbesserung der Angriffserkennung sollten die neuen Angriffs-Patterns als dynamische Filter-Regeln definiert und für zukünftige Traffic-Analyse hinterlegt werden.

Schutz für OSI-Layer

Im Allgemeinen können DDoS-Angriffe danach aufgegliedert werden, welche Ebene des Open Systems Interconnection (OSI)-Modells sie angreifen. Sie erfolgen am häufigsten auf den Ebenen Netzwerk (Ebene 3), Transport (Ebene 4) und Anwendung (Ebene 7). Effizienter DDoS-Schutz sollte daher bis zu Layer 7 reichen.

Application Layer (#7)
Die Herausforderung in der Angriffserkennung besteht darin, dass sich der DDoS-Traffic als legitimer Datenverkehr tarnt. Er kann auf die Überlastung von CPU und Datenbanken zielen, z. B. durch DDoS-Attacken auf Login-Seiten oder manipulierte Suchanfragen auf dynamischen Webseiten und Feedback-Seiten. Nimmt die DDoS-Schutzlösung aber eine Deep Packet Inspection vor, können die Informationen durch Einsatz von Maschinellem Lernen und Künstlicher Intelligenz für die Filterung des Datenverkehrs genutzt werden.
Bsp.: GET, TLS, HTTP GET, HTTP Post

Transport layer (#4)
Volumetrische Attacken, auch Floods genannt, belegen Bandbreite und sorgen dafür, dass Webseiten nur langsam oder gar nicht verfügbar sind.
Bsp.: UPD Floods, ICMP Floods, SYN Floods

Transport layer (#3)
Ebenfalls volumetrische Attacken, die Bandbreite und das Rate-Limiting der Firewall zu überlasten versuchen

Service Level Agreements

Die Service-Standards (Service Level Agreement/SLA) sind insgesamt in mehreren Einheiten definiert: Es gibt Service-Kategorien für das Schutzniveau, die Reaktionszeiten bei der Abwehr sowie für die generelle Netz- und Dienstverfügbarkeit.

SLA auf die Schutzbandbreite

Die Angriffsvolumen bei DDoS-Attacken variieren sehr stark und hängen zumeist von den eingesetzten Angriffsvektoren und Verstärker-Techniken (Reflection-Amplification-Attacks) ab. Die erzeugten DDoS-Bandbreiten sind in den vergangenen Jahren kontinuierlich gestiegen. Während der Mittelwert der Attacken 2016 noch bei 2 Gbps lag, erreichter er 2019 durchschnittlich 5,3 Gbps. Neben der mittleren Bandbreite ist auch das maximale Angriffsvolumen der DDoS-Attacken gestiegen. 2018 lag es bei 1,7 Tbps, 2019 bei 1,3 Tbps und im Februar 2020 bei 2,3 Tbps. Angedrohte Angriffe mit 2 Tbps durch international agierende und sehr aggressive DDoS-Erpresser wie die im August und September 2020 unter dem Namen „Fancy Bear“ und „Armada Collective“ agierenden Täter sollten angesichts dieser Entwicklung sehr ernst genommen werden.

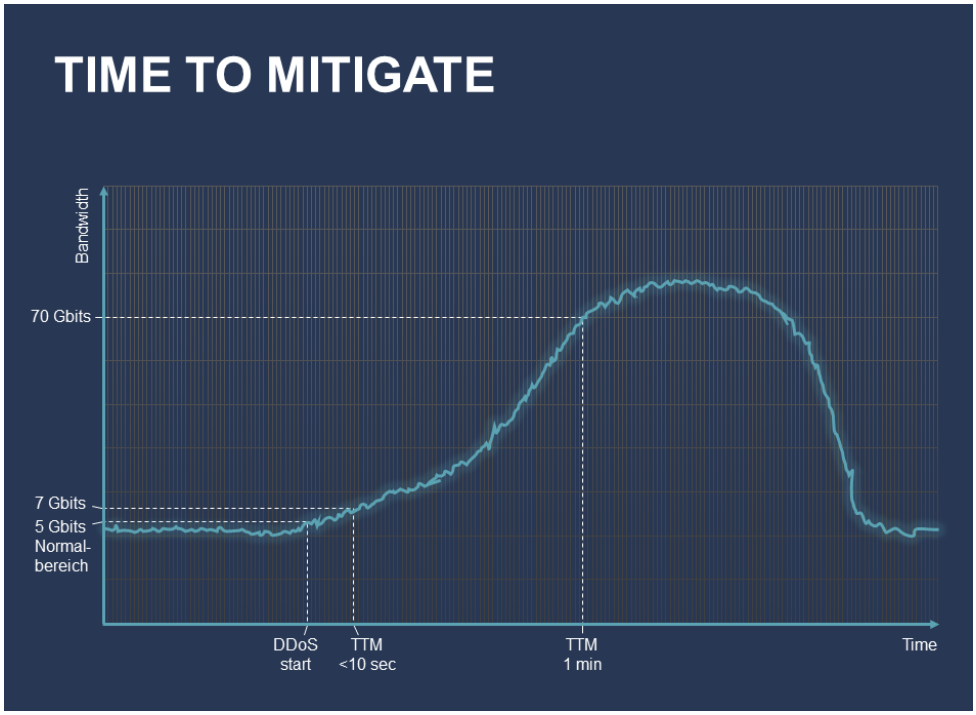
Die Entwicklung der Breitbandzugänge für Unternehmen hängt in weiten Teilen der Welt dem Volumenwachstum bei DDoS-Attacken hinterher. Erst ein Sechstel der Firmen in der EU nutzt schnelle Internetanbindungen von über 100 Mbps, die Mehrheit hat einen deutlich schmalbandigeren Anschluss. Für Unternehmen, die Schutz suchen, ist deshalb eine Schutzlösung wichtig, die deutlich größere Angriffsvolumen als die eigene Außenanbindung blocken kann. Gleichzeitig sollte sie flexibel skalierbar sein, um den immer größer werdenden Angriffen gewachsen zu sein. Ausgehend vom bisher größten bekannten Attacken-Volumen in Gbps als auch in packets per second (pps) sollte der DDoS-Schutzanbieter eine Schutzbandbreite, z. B. von 10 Gbps, 50 Gbps, 100 Gbps oder 500 Gbps garantieren.

Zum Schutz vor hochvolumigen Attacken sollte der DDoS-Schutzprovider ein weltweites Netzwerk betreiben. Eine große Außenanbindung ermöglicht es, Attacken von Dutzenden oder Hunderten Gbps aufzunehmen und zu filtern. Die globale Verteilung der Filter-Cluster trägt außerdem dazu bei, die Attacken möglichst nah am Ursprung zu filtern. Zu den wichtigsten Quellenländern für DDoS-Attacken zählen die USA, China, Russland sowie zahlreiche südamerikanische und europäische Länder.

SLA bei Time to Mitigate

Viele Online-Services und digitale Geschäftsmodelle wie Direktbanken oder Logistik versprechen den Nutzern Zugriff rund um die Uhr und ohne Unterbrechung. Übersetzt in die Anforderungen an den DDoS-Schutz bedeutet dies 100 Prozent.

Verfügbarkeit und Performance. Bei der Erkennung und Abwehr (Time to Mitigate) einer Attacke zählt daher jede Sekunde. Die TTM beginnt, wenn das erste DDoS-Angriffspaket das System erreicht, und dauert so lange, bis die DDoS-Schutzlösung die Bereinigung des Datenverkehrs startet. Einige Anbieter legen sich nur auf eine Time to Detection (TTD) fest und bleiben bei der zweiten Phase der Response Zeit, der Mitigation, unbestimmt. Für ein Unternehmen, das angegriffen wird, zählt aber allein, wann der Angriff gestoppt ist.



Wenn DDoS-Angriffe zu spät gestoppt werden, kann das Angriffsvolumen in der Infrastruktur des Kunden große Schäden anrichten.

Die TTM fällt bei den Schutzlösungen sehr unterschiedlich aus. Sie kann von 0 bis wenige Sekunden – also Echtzeit - bis hin zu 30 Minuten oder noch länger dauern. Zeitspannen von mehreren Minuten sind hierbei aufgrund nachgelagerter Effekte wie dem Zusammenbruch von IP-Tunneln, dem Rebooten von Servern etc. inakzeptabel. Nur die Bekämpfung der Angriffe in Echtzeit stellt sicher, dass Internetanbindungen nicht überlastet werden. Die TTM sollte außer für volumetrische auch für Attacken auf Applikationsebene (Layer 7) auf APIs und Applikationen gelten (siehe Kapitel „Schutz für OSI-Layer“). Da sich Layer-7Attacken als valide Pakete tarnen, sind sie schwieriger zu erkennen und zu blocken. Abwehrgarantien mit einem Service Level Agreement von 100 Prozent sollten außerdem nicht nur für ausgewählte, sondern für alle Angriffstechniken inklusive neuartiger Vektoren gelten

SLA bei Service Uptime

Die Service-Uptime garantiert, dass die Infrastruktur des DDoS-Schutzanbieters verfügbar bleibt und der Kunde unterbrechungsfrei geschützt ist. Digitalisierung duldet keine IT-Ausfälle. Downtimes schädigen zum einen den Ruf des Unternehmens, zum anderen verhindern sie Umsätze bzw. verursachen Betriebsunterbrechungen. Aus diesem Grund sollten Unternehmen von ihrem DDoS-Schutzanbieter ein Maximum an Service-Uptime einfordern. Dieser liegt als Branchenstandard zwischen 99,9 und 99,99 %. Nutzt ein Unternehmen die DDoS-Schutzlösung über seinen Hosting-Anbieter, sollte dieser eine Service-Uptime garantieren.

Skalierbarkeit der Gesamtlösung

Für Unternehmen wird es immer wichtiger, in eine DDoS-Schutzlösung zu investieren, die mit der Firmeninfrastruktur linear mitwachsen kann. Neue Standorte im weltweiten Unternehmensnetzwerk, Ausbau der Applikationen und steigende Nutzung von APIs – dies sind nur einige von vielen möglichen Treibern, die ein Aufstocken des DDoS-Schutzes notwendig machen. Bei appliance-basierten Lösungen bedeutet dies Reinvestitionen in Form von Zukäufen und erfordert teils eine mehrmonatige Vorlaufzeit. Cloudbasierter Schutz lässt sich hingegen kurzfristig und flexibel um neue Instanzen erweitern – ohne Anschaffung von Hardware. Die Kosten verhalten sich linear zur Nutzung (siehe Kapitel „Preisgestaltung“).

Angesichts steigender Angriffsvolumen von mehreren 100 Gbps oder getrieben durch akute Vorfälle wie Erpresserwellen sollte außerdem regelmäßig geprüft werden, ob die gebuchte Schutzbandbreite noch angemessen ist. Bei DDoS-Schutz aus der Cloud, der mit einem weltweiten Netzwerk ausreichend Ressourcen vorhält, kann zusätzlicher Schutz in kürzester Zeit bereitgestellt werden. Auch im akuten Angriffsfall kann eine kurzfristige Skalierung notwendig werden: Übersteigt ein

Angriff beispielsweise die Schutzbandbreite, muss sich diese jederzeit und schnell erweitern lassen. Appliances sind hierbei durch die maximal verfügbare Außenanbindung limitiert, siehe Kapitel „Lösungsansätze im DDoS-Schutz“.

Multicloud Support

Unternehmen setzen immer stärker auf hybride IT-Landschaften, die sich aus eigenen Rechenzentren, Web-Services sowie Anwendungen in der Privat- und Public-Cloud zusammensetzen. Um Risiken zu reduzieren, sollten die Firmen dieselben Sicherheitsstandards über alle ihre digitalen Arbeits- und Geschäftsumgebungen hinweg anstreben. Da jede Cloud beim DDoS-Schutz anderen Standards folgt, droht ein komplex verteiltes Security-Problem in der Multi-Cloud. Der hohe administrative Aufwand geht mit einem uneinheitlichen Schutzniveau einher, das die IT-Sicherheit eher schwächt als stärkt.

Um die Komplexität und die hohen Anforderungen an Verfügbarkeit und Performance sicher zu managen, sind komplette DDoS-Schutzlösungen aus einer Hand ein guter Weg. Es hat sich bewährt, den Schutz über alle genutzten Cloud-Plattformen auszurollen. Sowohl aus technischer als auch aus sicherheitsrelevanter und Compliance-Sicht entsteht somit ein konsistenter und zuverlässiger Schutz der gesamten Unternehmens-IT. Er ist unabhängig vom Cloud-Anbieter, maßgeschneidert für das Unternehmen und bleibt flexibel für Skalierungen in der Cloud-Nutzung. Multinationale Unternehmen mit weltweit verteilten Standorten profitieren beim Schutz ihrer Infrastrukturen zudem von einer niedrigen Latenz.

Compliance

Bei der Absicherung digitaler Geschäftsprozesse müssen Unternehmen verschiedene Regularien auf nationaler und internationaler Ebene beachten wie DSGVO und BDSG. Eine Rundumlösung, die sowohl DDoS-Schutz als auch Rechtskonformität gewährleistet, ist der beste Weg. Probleme tauchen häufig dann auf, wenn sich Server-Standorte des Schutzanbieters etwa außerhalb des Geltungsbereiches der EU-DSGVO befinden. Auch Subunternehmer seitens des Schutzanbieters können für Compliance-Bedenken sorgen: Wenn Dienste der eingesetzten Schutzlösung an externe Unternehmen ausgelagert werden, kann dies die Transparenz enorm herabsetzen – insbesondere im Hinblick auf die Einhaltung rechtlicher Anforderungen.

Das Aus für den EU-US Privacy Shield durch den Europäischen Gerichtshof im Juli 2020 verschärfte die Compliance-Anforderungen an DDoS-Schutzlösungen, deren Anbieter nicht aus dem EU-Raum stammen. Im Rahmen von CDN-basierten Produkten werden oft standardmäßig Metadaten aus der EU-Datenschutzzone in die USA übertragen. Zudem speichern die Diensteanbieter vielfach Logfiles auf US-amerikanischem Territorium und nutzen sie innerhalb ihres Network Operation Centers (NOC) für weitreichende Optimierungen der eingesetzten Systeme oder zur besseren Einstufung der Bedrohungslage. Darüber hinaus können die wertvollen Metadaten auch in die Arbeit zentral geführter Security Operation Centers (SOC) einfließen. Diese werten sie zur Gefahrenerkennung und Schärfung der relevanten Filter und Schutzmechanismen aus. Allzu oft jedoch befinden sich das NOC und das SOC außerhalb der EU, z. B. in den USA. Die Problematik der Datenübertragung und -speicherung trifft vielfach auch auf Anbieter von Hardware-Appliances zu.

Unternehmen, die auf Nummer sicher gehen möchte, sollten ihre Daten und IT-Sicherheit einem Anbieter aus Deutschland bzw. Europa anvertrauen und damit eine Datenübertragung in die USA von vornherein ausschließen. Die strengen Vorgaben des europäischen und des deutschen Gesetzgebers zum Datenschutz und zur Datensicherheit bieten die erforderliche Sicherheit für eine Datenübermittlung. Meist wird dadurch auch die Einhaltung von Compliance-Anforderungen erleichtert. Sicherheitshalber sollte man einen Dienstleister ohne Niederlassung in den USA wählen, um einen etwaigen Zugriff der US-Niederlassung auszuschließen. EU-Anbieter ohne US-Niederlassungen sind außer mit rechtlichen Aspekten vielfach auch mit technologischen Vorteilen verbunden. Zudem verfügen sie über umfassende und profunde Kenntnisse bezüglich des europäischen Marktes sowie bezüglich der Bedürfnisse ihrer europäischen Kunden.

Dashboard mit Konfigurationsmöglichkeiten

Transparenz und Monitoring des Webseiten- und Netzwerkverkehrs sollten über ein webbasiertes Dashboard gewährleistet werden. Neben den Einstellungsmöglichkeiten für kundenspezifische Schutzparameter liefert es Echtzeitanalysen des Datenverkehrs und protokolliert Detailinformationen zu abgewehrten DDoS-Attacken:

- detailliertes Reporting
- Konfiguration der Blacklist/Whitelist
- Einrichtung der statischen Filterregeln
- Management der weltweit verteilten Schutz-Infrastruktur und unterschiedlicher Schutzprofile
- Alert-Funktion
- Individuelle Einstellungsmöglichkeiten

Preisgestaltung und Kosten

Es existieren mehrere Preismodelle, um DDoS-Schutzleistungen zu berechnen. Der Konsum der IT-Sicherheitsleistungen wird dabei in Investitionen in Anlagevermögen (Capex) und Betriebsausgaben (Opex) erfasst. Je nach Wahl der Schutzlösung stehen Capex und Opex unterschiedlich zueinander im Verhältnis und können ein finanzielles Risiko darstellen:

Hardware Appliances

- hoher Capex- und Opex-Anteil
- hohe Ausgaben für Kauf der Appliances
- Folgekosten, die durch Aktualisierung/Austausch der Appliances im Turnus von x Jahren entstehen
- zusätzliche Anschaffungskosten, wenn das Unternehmen und damit die zu schützende Infrastruktur wächst
- hoher Bedarf an spezialisierten IT-Managern und Support-Mitarbeitern für Wartung und Weiterentwicklung
- hohe Investitionen in eigene IT-Infrastruktur (Rechenzentren, Server, Netzwerke)
- Gebühren für Schulungen, Support und Updates kommen meist noch hinzu.

CDN-basierter Schutz

- geringe Capex-Kosten, hohe Opex-Ausgaben
- bei der Nutzung von CDN-Services zur Absicherung gegen DDoS-Attacken werden keine Investitionskosten in Hardware fällig
- die Abrechnung erfolgt nach Verbrauch: Traffic-Durchsatz pro Sekunde (Mbit/s) oder Volumen pro Monat (Tbyte/Monat)
- die Kosten sind erheblich geringer als bei einer klassischen On-Premise-Lösung

Cloudnativer Ansatz (AWS/Azure)

- niedriger Capex-Anteil, ebenfalls niedrige Opex-Kosten für Standardschutz
- Advanced-Schutz gegen komplexe Attacken nur gegen Aufpreis
- Abrechnung auf Monatsbasis
- Angriffe werden zum Teil berechnet (burst capacity)

Cloud-Schutz

- Angriffe werden zum Teil berechnet (burst capacity)
- niedriger Capex-Anteil, ebenfalls niedrige Opex-Kosten
- standardmäßig wird Cloud-Schutz im Rahmen von Monats- oder Jahresverträgen berechnet
- geringe Kapitalbindung in Hardware und Software, abhängig von Deployment-Modell DNS Forwarding oder BGP Forwarding

- geringer Bedarf an IT-Managern und Supportmitarbeitern für Wartung
- Abrechnung nach entstandener Nutzung, die sich z. B. nach der garantierten Schutzbandbreite richtet, am Clean-Traffic orientiert oder auf der Anzahl der zu schützenden Instanzen (IPs, Webseiten, Rechenzentren) basiert
- Ggf. kommen Gebühren für die Implementierung und den Support hinzu
- Einige Anbieter verlangen zusätzliche Gebühren, wenn der Angriff eine bestimmte Zeitdauer oder eine festgelegte Anzahl übersteigt. Das macht es für Kunden schwierig, die Kosten abzuschätzen.

Neben den Kosten muss auch die Flexibilität betrachtet werden. Bei der Nutzung von DDoS-Schutz aus der Cloud herrscht Unabhängigkeit: Der DDoS-Schutz kann bei planbaren monatlichen Kosten flexibel mit dem Unternehmen mitwachsen. Außerdem bestehen kurze Laufzeiten für die Nutzung. Hardware-Lösungen, die als Investitionen betrachtet werden, rentieren sich erst nach einer längeren Laufzeit.

Integrierte Plattform für DDoS-nahe Dienste

Für die vollumfängliche Absicherung von Performance und Verfügbarkeit auf Netzwerk- und Applikationsebene kann die Kombination von DDoS-Schutz mit weiteren IT-Sicherheitslösungen sinnvoll sein. Folgt man einem 360-Grad-Ansatz, lässt sich z. B. durch den Einsatz einer Web Application Firewall oder von Secure DNS Services die Sicherheit weiter steigern. Eine vollständig integrierte Lösung bei einem einzigen Anbieter hilft, wichtige Sicherheitslücken zu schließen. Darüber hinaus gilt: Je mehr Anwendungen in einer Managementkonsole (Single Pane of Glass) zusammengefasst werden, desto effizienter unterstützen sie die Absicherung von Netzwerken und Applikationen:

- Dienste sind aufeinander abgestimmt und verzahnt
- Die eingesetzten Schutzfunktionen lassen sich bedarfsgerecht erweitern
- Die Integrierbarkeit mit APIs ermöglicht die Einbindung in die bestehende IT-Infrastruktur des Unternehmens
- Weniger Schulungs- und Verwaltungsaufwand (Administration)

Der ineffektive und oft wenig kostengünstige Parallelbetrieb mehrerer Lösungen ist mit der Entscheidung für eine Plattform Vergangenheit.

Support

Der Schutz vor DDoS-Attacken wird erst durch fachlich versierten Support, der gut erreichbar ist, ganzheitlich:

- Verfügbarkeit 24/7
- Kommunikation per Telefon, E-Mail oder Chat
- in Landessprache
- über einen zugeordneten Customer Success Manager.
- Reaktionszeiten bzw. Antwortzeiten sind bei vielen Anbieten in den SLA definiert und reichen von 30 Minuten bis hin zu mehreren Stunden.

Darüber hinaus begleiten die Support-Mitarbeiter die Implementierung, unterstützen den Kunden beim Einrichten der Schutzlösung, z. B. bei der Umleitung des Datenverkehrs, sowie bei der Bereitstellung des bereinigten Datenverkehrs für den Kunden und beraten proaktiv bei der Integration in die bestehende IT-Sicherheitsinfrastruktur.

Außerdem berät der Support die DDoS-Schutzkunden beim Umgang mit DDoS-Erpressungen.

Fazit

DDoS-Attacken gehören heute für immer mehr Unternehmen zur alltäglichen Bedrohung. In Zeiten zunehmender Digitalisierung und immer größer werdenden Angriffsflächen in der IT-Infrastruktur müssen sie sich auf Angriffe einstellen, die in Zukunft noch großvolumiger und komplexer ausfallen. Der Trend zu einer verstärkten Nutzung von Anwendungen in der Cloud bietet weitere Einfallstore und wird zu einem weiteren alarmierenden Anstieg von DDoS-Attacken auf Layer 7 führen.

Aus diesem Grund ist effektiver DDoS-Schutz unerlässlich. Das Wissen um die Bedrohungen und um die verschiedenen Technologien, die Unternehmen zur Verfügung stehen, helfen, eine fundierte Entscheidung zu treffen und den besten Schutz vor heute schon bekannten und zukünftigen Angriffen zu finden.

Über Link11

Link11 ist der im Bereich Cyber-Resilienz führende europäische IT-Sicherheitsanbieter. Die globalen Schutzlösungen der Cloud Security Plattform sind vollständig automatisiert, reagieren in Echtzeit und wehren alle Angriffe, so auch unbekannte und neue Muster, in unter 10 Sekunden ab. Link11 bietet laut einhelliger Analysten-Meinung (Gartner, Frost & Sullivan) die schnellste Mitigation (TTM), die auf dem Markt verfügbar ist. Um Cyber-Resilienz zu gewährleisten, sorgen u.a. Web- und Infrastruktur-DDoS-Schutz, Bot-Mitigation, API-Schutz, Secure-DNS, Zero-Touch-WAF, Secure-CDN bis hin zu Threat-Intelligence-Services für eine ganzheitliche und Plattform-übergreifende Härtung der Netzwerke und kritischer Anwendungen von Unternehmen. Die internationalen Kunden können sich so auf ihr Geschäft und digitales Wachstum konzentrieren. Seit der Gründung des Unternehmens im Jahr 2005 wurde Link11 mehrfach für seine innovativen Lösungen ausgezeichnet.

Link11 GmbH
Lindleystraße 12
60314 Frankfurt Germany
+49 (0)69 - 264929777
info@link11.com

Checkliste

Auf welche Punkte ist bei der Auswahl eines DDoS-Schutzanbieters zu achten? Der Kriterienkatalog hilft Ihnen, die Verlässlichkeit und Vertrauenswürdigkeit verschiedener Schutzlösungen zu beurteilen.
Zum Ausdrucken und Ausfüllen!

Feature	Link11	Anbieter 1	Anbieter 2
Garantierte Schutzbandbreite	✔		
Garantierte Abwehrzeit, die alle Vektoren und Layer einschließt	✔		
Garantierte Verfügbarkeit (Service Uptime)	✔		
Verfügbarkeit als Web-Schutz/ DNS Forwarding	✔		
Infrastrukturschutz via BGP on-demand	✔		
Infrastrukturschutz via BGP always on	✔		
Flexible Kombinationsmöglichkeiten aus Web- und Infrastrukturschutz	✔		
Hybride Schutzlösung (Cloud u. Appliance)	✔		
Statische Filter-Regeln (TCP, UDP, ICMP, IPs, Rate-Limits etc.)	✔		
Schutz auf Layer 3-7	✔		
Dynamische Filterregeln (Whitelisting auf Basis KI)	✔		
Automatisierte Prozesse und Filterung	✔		
Multicloud-Support	✔		
Integrierte Plattform für DDoS-nahe Web-Security-Dienste	✔		
SaaS-Geschäftsmodell reduziert Investitionsrisiken	✔		
Keine Zusatzkosten abhängig von der Angriffsdauer	✔		
Skalierbarkeit des Schutzes	✔		
Eigenes, selbst gemanagtes weltweites Filternetzwerk	✔		
DSGVO-konform	✔		
EU-rechtskonform (insbesondere mit Urteil des EuGH zu Privacy Shield)	✔		
Dashboard mit Konfigurationsmöglichkeiten	✔		
Deutschsprachiger Service für Implementierung u. Setup	✔		
24/7-Servicecenter in Deutschland	✔		