LINK11

DDOS PROTECTION BUYER'S GUIDE

Worauf sollte man bei einer DDoS-Schutzlösung achten

www.link11.com

Die Wahl der richtigen Lösung zum Schutz Ihres Unternehmens vor Distributed Denial-of-Service (DDoS)-Angriffen, die zu schädlichen Geschäftsunterbrechungen führen können, ist in der heutigen digitalen Landschaft von entscheidender Bedeutung. Eine effektive Lösung entschärft nicht nur Angriffe, sondern gewährleistet auch die ununterbrochene Verfügbarkeit und Leistung Ihrer wichtigsten Dienste. Angesichts der zunehmenden Komplexität und Häufigkeit von DDoS-Bedrohungen ist die Auswahl des richtigen Schutzes wichtiger denn je.

Die Produkte der Anbieter von DDoS-Diensten und -Lösungen können sich erheblich unterscheiden, was die Auswahl der richtigen Schutzlösung zu einer Herausforderung macht. In diesem Leitfaden erfahren Sie, worauf Sie bei der Bewertung von DDoS-Schutzoptionen achten sollten, und erfahren, welche Vorteile die Zusammenarbeit mit einem externen Sicherheitsanbieter bietet. Außerdem werden die grundlegenden Funktionen moderner DDoS-Schutzlösungen erläutert - Fragen, die Sie mit potenziellen Anbietern besprechen sollten.

In diesem Leitfaden werden wir bewährte Verfahren zur Bewertung von DDoS-Schutzlösungen und zur Auswahl derjenigen Lösung besprechen, die einen ganzheitlichen Ansatz zur Sicherung Ihrer Arbeitslasten bietet, skalierbar ist, um zukünftige Geschäftsanforderungen zu erfüllen und sich an neu auftretende Bedrohungen anpasst.

Wichtige Kriterien für die Bewertung von DDoS-Schutzlösungen

Bei der Überprüfung von DDoS-Schutzlösungen sollten Sie folgende Kriterien berücksichtigen:

1. Verfügbare DDoS-Schutzlösungen
2. Routing-Lösungen: Umleitung des Datenverkehrs
3. Verfügbarkeit: „Always-On“ oder „On-Demand“
4. Filteroptionen
5. Automatisierung bei der Angriffserkennung und -filterung
6. Schutz für OSI-Layer
7. Multi-Cloud-Unterstützung
8. Compliance
9. Überwachung und Visualisierung
10. Integrierte Plattform für DDoS-bezogene Dienste
11. Support und verwaltete Dienste

1. VERFÜGBARE DDOS-SCHUTZLÖSUNGEN

Organisationen nutzen verschiedene Ansätze, um sich gegen DDoS-Angriffe zu verteidigen, darunter Hardware-Anwendungen (On-Premises), cloud-basierte und cloud-native Lösungen sowie hybride Schutzmodelle.

a) Anwendungen / On-Premises

Die Anwendung überwacht den Datenverkehr und schränkt böswillige Anfragen ein oder blockiert sie, wenn Anomalien wie ein Anstieg des Datenverkehrs festgestellt werden. Bei einigen Bereitstellungsmodellen ist ein manuelles Eingreifen von IT-Teams oder externen Sicherheitsanbietern erforderlich.

- **Anpassung:** Bietet maßgeschneiderte Anpassungen an spezifische IT-Infrastrukturen und Datenverkehrsmuster.
- **Datenschutz:** Sensible Informationen bleiben im Netzwerk der Organisation und werden nicht an Dritte weitergegeben.
- **Einschränkungen der Skalierbarkeit:** Hardware-Anwendungen können mit großangelegten Angriffen, die ihre Kapazität übersteigen, Probleme haben.
- **Hohe Kosten:** Erfordert erhebliche Vorabinvestitionen für Beschaffung, Wartung und Updates.
- **Wartungskomplexität:** Erfordert internes Fachwissen für die Verwaltung und Aktualisierung.
- **Begrenzte Abdeckung:** Die Effektivität kann bei geografisch verteilten Infrastrukturen oder externen Vermögenswerten abnehmen.

b) Cloud-basierter DDoS-Schutz

Bei diesem Ansatz wird der Datenverkehr der Website durch den externen Filter des Anbieters geleitet, sodass eine mehrschichtige Analyse zur Erkennung und Blockierung von Angreifern möglich ist. Nur legitimer Datenverkehr wird weitergeleitet.

- **Skalierbarkeit:** Verwaltet großangelegte Angriffe mithilfe einer verteilten Cloud-Infrastruktur.
- **Einfache Bereitstellung:** Schnelle Einrichtung mit minimalem technischem Aufwand.

- **Globale Reichweite:** Schützt Assets in einer Vielzahl von Regionen ohne zusätzliche Hardware.
- **Umfassende Angriffserkennung:** Wirksam gegen volumen-, anwendungs- und protokollbasierte Angriffe sowie unbekannte Vektoren.
- **Probleme mit der Datensouveränität:** Kann aufgrund der Datenweiterleitung durch Dritte zu regulatorischen Bedenken führen.
- **Anbieterabhängigkeit:** Nach der Integration kann es schwierig sein, den Anbieter zu wechseln

c) Cloud-nativer DDoS-Schutz

Cloud-native DDoS-Schutzlösungen sind für eine schnelle Implementierung ausgelegt und verfügen über eine Reihe grundlegender Optionen und Sicherheitseinstellungen. In der Praxis erweisen sich diese Lösungen jedoch oft als unzureichend, um Anwendungen und Daten in Produktionsumgebungen **vollständig zu schützen**. Da die Benutzer für die Sicherheit und den Datenschutz verantwortlich bleiben, wenn sie sich auf Dritte verlassen, sind erhebliche Anpassungen und spezielles Fachwissen erforderlich.

- **„Built-In"-Integration:** Speziell für Cloud-Umgebungen entwickelt, nahtlose Integration in cloud-native Anwendungen.
- **Dynamische Skalierbarkeit:** Passt sich automatisch an, um auf ein wachsendes Angriffsvolumen zu reagieren.
- **Geringe Latenz:** Reduziert Verzögerungen bei der Umleitung durch die Integration in das Netzwerk des Cloud-Anbieters.
- **Einhaltung gesetzlicher Vorschriften:** Einige Anbieter bieten an die Compliance angepasste Lösungen an, die auf bestimmte regionale Gesetze und Vorschriften zugeschnitten sind.
- **Sicherheitskosten:** Erweiterter Schutz ist oft mit hohen Kosten verbunden, die über die Grundabdeckung hinausgehen.
- **Begrenzte Anbieteroptionen:** Oft an bestimmte Cloud-Anbieter gebunden, was die Flexibilität einschränkt.
- **Kostenabhängigkeit von der Cloud-Nutzung:** Die Preise richten sich nach der Cloud-Nutzung, was die Kosten für Anwendungen mit großem Datenverkehr erhöhen kann

d) Hybride Schutzlösungen

Dieser kombinierte Ansatz integriert Hardware- und cloud-basierte Lösungen für einen umfassenden Schutz vor Angriffen auf Anwendungs- und Netzwerkebene.

- **Umfassende Abdeckung:** Bietet robusten Schutz durch die Kombination von lokalen und cloud-basierten Funktionen.
- **Flexibilität:** Verarbeitet kleinere Angriffe lokal, während Cloud-Lösungen für großangelegte Bedrohungen skaliert werden können.
- **Hohe Bandbreitenstärke:** Effektiv für die Skalierung, aber durch die Kapazität der Hardware begrenzt.
- **Integrationskomplexität:** Die Integration in bestehende IT-Infrastrukturen ist schwierig.
- **Verzögerungen beim Wechsel:** Kann zu Latenz oder Ausfallzeiten während Angriffen führen.
- **Compliance-Probleme:** Es müssen die Datenschutzstandards des Landes eingehalten werden.
- **Höhere Gesamtkosten:** Die Kombination von Lösungen erhöht die Kosten im Vergleich zu eigenständigen Ansätzen.

2. ROUTING-LÖSUNGEN: UMLEITUNG DES DATENVERKEHRS

DDoS-Schutz kann über DNS-Weiterleitung oder während eines Angriffs durch Weiterleitung des Datenverkehrs über BGP an den Schutzanbieter oder seine Scrubbing-Center zur Filterung implementiert werden. Die Struktur der IT-Systeme des Unternehmens spielt bei der Wahl zwischen diesen beiden Routing-Lösungen eine entscheidende Rolle.

a) DDoS-Schutz durch DNS-Weiterleitung

DNS-Schutz zielt darauf ab, die Webanwendungen eines Unternehmens zu sichern, ohne dass die Serverinfrastruktur erweitert, die Bandbreite erhöht oder neue Router-Technologie gekauft werden muss. Die Implementierung kann bereits mit nur einer IP-Adresse erfolgen. Diese Methode schützt Anwendungen, die auf Domainnamen basieren, vor DDoS-Angriffen auf Layer 7.

Dazu werden die DNS-A-Record-Einträge der betroffenen Anwendung so geändert, dass der Datentransfer zum Scrubbing-Center umgeleitet wird. Infizierte Clients fragen die DNS-Server nach der IP-Adresse ab, erhalten die IP-Adresse des Scrubbing-Centers über die DNS-Änderung und vermeiden so, den Angriff an den ursprünglichen Server zu senden. Der Schutz ist aktiv, sobald die DNS-Serveränderung vorgenommen wurde.

b) DDoS-Schutz über das Border-Gateway-Protocol (BGP)

Der BGP-DDoS-Schutz, auch bekannt als Layer-3- und Layer-4-DDoS-Schutz, kann in einem Hot-Standby-Modus verwendet werden, der den normalen Datenfluss aufrechterhält, wenn kein Angriff erkannt wird. Im Falle eines Angriffs wird der Datenverkehr durch das Scrubbing-Center geleitet. Die gefilterten Datenpakete werden dann über einen geschützten Tunnel (VPN, IPsec, GRE) an das Netzwerk des Kunden zurückgesendet.

Sobald der Angriff abgewehrt ist, wird der Datenverkehr auf die ursprüngliche Route umgeleitet. Eine BGP-Lösung erfordert ein 24-IP-Netzwerk oder größer für die Umleitung. Vollständige Protokolle können auch gemäß den Kundenspezifikationen weitergeleitet werden. Während eines Angriffs können sowohl der Kunde als auch das Sicherheitskontrollzentrum das Netzwerk in einer Standby-Integration ankündigen.

c) Mögliche Kombinationen: Web-DDoS und Infrastruktur-Schutz

Da die IT-Infrastrukturen von Unternehmen immer komplexer werden und aus Webservern, Datenbanken, Internet-Telefonie und Cloud-Anwendungen bestehen, wird für einen maximalen DDoS-Schutz häufig eine Kombination aus DNS-Weiterleitung und BGP-Umleitung empfohlen. Die Wahl sollte immer auf die spezifischen Bedürfnisse des Unternehmens zugeschnitten sein und auf einer gründlichen Analyse mit dem DDoS-Schutzanbieter basieren.

3. VERFÜGBARKEIT: ALWAYS-ON ODER ON-DEMAND

Bei der Auswahl einer DDoS-Schutzlösung ist eine der wichtigsten Entscheidungen, ob ein Always-On- oder ein On-Demand-Schutz gewählt werden soll. Beide Ansätze bieten einzigartige Vorteile und eignen sich für unterschiedliche Geschäftsanforderungen, Branchen und Bedrohungslandschaften. Always-On-Schutz gewährleistet eine kontinuierliche, automatisierte Verteidigung gegen alle Arten von DDoS-Angriffen und bietet maximale Betriebszeit und Zuverlässigkeit.

Der On-Demand-Schutz hingegen wird nur aktiviert, wenn eine Bedrohung erkannt wird, und bietet Kosteneffizienz bei gleichzeitiger Aufrechterhaltung einer robusten Sicherheit. Das Verständnis der Unterschiede zwischen diesen Ansätzen ist wichtig, um eine fundierte Entscheidung zu treffen, die mit den Sicherheitsprioritäten und dem Budget Ihres Unternehmens übereinstimmt.

a) On-Demand Schutz

Der On-Demand-DDoS-Schutz ist eine flexible Lösung, die volumetrische und protokollbasierte Angriffe (Layer 3/4) abwehren kann. Unter normalen Bedingungen fließt der Kundenverkehr ununterbrochen und wird mithilfe von Flussdaten, Telemetrie oder anderen Analysen kontinuierlich überwacht. Wenn ein Angriff erkannt wird, wird der Dienstanbieter oder Kunde alarmiert und der Datenverkehr wird zur Entschärfung an ein Scrubbing-Center umgeleitet.

Diese Umleitung wird durch BGP (Border Gateway Protocol) -Ankündigungen ermöglicht, die manuell durch den Kunden oder automatisch durch den Anbieter ausgelöst werden können. Nach der Umleitung filtert das Scrubbing-Center den bösartigen Datenverkehr heraus und stellt sicher, dass nur sauberer Datenverkehr über vorkonfigurierte Tunnel, wie z. B. GRE (Generic Routing Encapsulation) -Tunnel, an den Kunden weitergeleitet wird.

Ein wesentlicher Vorteil des On-Demand-Schutzes ist seine Flexibilität. Die Kunden erhalten eine größere Kontrolle über das Netzwerk-Routing und können so die Einleitung und Beendigung von Schutzmaßnahmen entsprechend ihren spezifischen Anforderungen steuern. Diese Kontrolle ist besonders wertvoll für Unternehmen mit komplexen oder dynamischen Routing-Anforderungen.

Der On-Demand-Schutz kann zwar die Kosten senken, indem er die Durchsatzgebühren minimiert oder Überschreitungsgebühren vermeidet, der Hauptvorteil besteht jedoch darin, dass der Schutz nur bei Bedarf aktiviert werden kann. Dieser Ansatz minimiert Unterbrechungen und optimiert die Netzwerkleistung in angriffsfreien Zeiten.

Wie bei jeder On-Demand-Lösung gibt es in der Regel eine kurze Verzögerung - oft nur wenige Minuten - bevor der Schutz vollständig aktiviert wird, da die Zeit für die Umleitung des Netzwerks benötigt wird. Bei wiederholten oder länger andauernden Attacken muss der Datenverkehr für jeden neuen Angriff neu angemeldet werden. Sobald der Angriff abgeklungen ist, wird der normale Datenverkehr wieder aufgenommen, so dass die Auswirkungen auf den Betrieb minimal sind. Dies macht den On-Demand-DDoS-Schutz zur idealen Wahl für Unternehmen, die eine reaktionsschnelle und anpassbare Schutzmaßnahme suchen.

b) Always-On Schutz

Mit dem Always-On-Schutz, sowohl über DNS-Weiterleitung als auch BGP-Umleitung, wird der Datenverkehr kontinuierlich durch ein Scrubbing-Center geleitet. Dieser Ansatz gewährleistet einen zuverlässigen Schutz für die IT des Unternehmens rund um die Uhr, an 365 Tagen im Jahr.

Die permanente Filterung und Bereinigung des Datenverkehrs reduzierten auch die Belastung der IT-Infrastruktur des Unternehmens. Diese kontinuierliche Überwachung minimiert das Risiko von Ausfallzeiten, gewährleistet einen unterbrechungsfreien Geschäftsbetrieb und garantiert das Vertrauen der Benutzer. Darüber hinaus ermöglicht der Always-On-Schutz eine schnellere Reaktion auf Bedrohungen und neutralisiert Angriffe effektiv, bevor sie sich auf das Netzwerk oder die Dienste des Unternehmens auswirken können.

Anbieter von DDoS-Schutzlösungen sollten flexible Bereitstellungsmodelle anbieten. Eine Kombination aus Always-On- und On-Demand-Lösungen kann den unterschiedlichen Schutzanforderungen komplexer Infrastrukturen gerecht werden. So können Unternehmen beispielsweise den Always-On-Schutz für ihre Anwendungen nutzen und ihn mit einem ereignisgesteuerten On-Demand-Schutz für E-Mail- und Datenbankserver kombinieren.

4. FILTER OPTIONEN

Es gibt zwei Hauptmethoden zum Filtern des Datenverkehrs: statische heuristikbasierte Filterung und dynamische heuristikbasierte Filterung.

a) Statische Analyse

Statische Filter verwenden vordefinierte Regeln (Blacklists), um den Datenverkehr zu überprüfen. Die Blacklist enthält Filterregeln für bekannte Angriffstypen. Wenn beim Vergleich der Verhaltensmuster bestimmter Anfragen Übereinstimmungen mit den Heuristiken der Blacklist auftreten, wird der Datenverkehr als DDoS eingestuft.

Zu den typischen Regeln für statische Filter gehören:

- Protokoll (TCP, UDP, ICMP usw.)
- TCP-Flags, ICMP-Typ
- Quell- und Ziel-IP
- Ratenbegrenzung pro IP oder Netzwerkbereich

Die Filterung von DDoS-Verkehr mithilfe statischer Regeln ist nur so effektiv wie die Blacklist, auf der sie basiert. Bei bestimmten oder neuen Arten von Angriffen kann es vorkommen, dass das System sie nicht als Bedrohung erkennt.

b) Dynamische Analyse

DDoS-Angreifer entdecken ständig neue Schwachstellen und offene Dienste, die für Überlastungsangriffe ausgenutzt werden können. Die jüngsten Memcached- und CLDAP-Angriffe sowie das Aufkommen der Vektoren WS-Discovery, Apple Remote Control und DVR DHCP Discovery zeigen, dass Unternehmen regelmäßig mit neuen Angriffstechniken konfrontiert sind.

Die Zukunft des Filterns liegt in Methoden, die proaktiv nach verdächtigen, aber undefinierten Verhaltensmustern suchen. Während normaler Datenverkehrszeiten lernt die Schutzlösung das legitime Datenverkehrsprofil einer Website oder eines Netzwerks und leitet daraus normale Bereiche (Whitelist) ab. Abweichungen und ungewöhnliche Verhaltensweisen werden dann automatisch durch maschinelles Lernen erkannt, wodurch Schäden verhindert werden, bevor sie entstehen.

5. AUTOMATISIERUNG BEI DER ERKENNUNG UND FILTERUNG VON ANGRIFFEN

Menschliches Versagen ist eine der Hauptursachen für Sicherheitsverletzungen. Bei der zunehmenden Anzahl von Alarmmeldungen können kritische Ereignisse leicht übersehen werden. Um eine Echtzeitreaktion und eine 100-prozentige Erkennung sowohl bekannter als auch bisher unbekannter Angriffe zu erreichen, müssen schnelle und zuverlässige Analyseprozesse hochgradig automatisiert sein. Eine effektive DDoS-Schutzlösung verwendet fortschrittliche, adaptive Filter, die auf legitimen Website-Verkehr kalibriert sind. Anstatt sich auf statische Ausschlussmethoden zu verlassen, nutzen diese Filter statistische Verhaltensmodelle, um ungewöhnliche IP-Aktivitäten zu erkennen und zu blockieren, wodurch die Anzahl der Fehlalarme minimiert wird. Während die Blacklist früher der Standard war, gewinnt die Whitelist an Bedeutung, indem sie Datenverkehr, der von etablierten legitimen Mustern abweicht, als potenziell schädlich kennzeichnet.

DDoS-Schutzlösungen sollten eingehenden Datenverkehr auf einer granularen Ebene analysieren und einen verfeinerten Ansatz bieten, der über eine einfache IP-basierte Identifizierung hinausgeht. Dadurch können reguläre Benutzer während eines Angriffs nahtlos auf Systeme zugreifen, ohne den Filterprozess überhaupt zu bemerken.

Eingehender Datenverkehr sollte mit historischen Angriffsdaten verglichen werden. Bei der Erkennung eines Angriffs wird nur der bösartige Datenverkehr blockiert, während legitime Daten weiterhin durch globale Filtercluster geleitet werden. Dadurch wird der Datenverkehr vollständig ausgelagert, sodass eine nahtlose Filterung im Hintergrund möglich ist, die von den Benutzern unbemerkt bleibt. Um die zukünftige Erkennung zu verbessern, sollten neue Angriffsmuster als dynamische Filterregeln gespeichert werden.

6. SCHUTZ FÜR OSI-LAYERS

DDoS-Angriffe lassen sich nach den Schichten des OSI-Modells (Open Systems Interconnection) aufschlüsseln, auf die sie abzielen. Die meisten Angriffe erfolgen auf der Netzwerk- (Layer 3), Transport- (Layer 4) und Anwendungsebene (Layer 7). Ein effizienter DDoS-Schutz muss bis zur Schicht 7 reichen.

Anwendungsschicht (#7)

Die Erkennung von Angriffen auf Layer 7 ist schwierig, da DDoS-Datenverkehr legitime Daten imitiert. Er kann beispielsweise versuchen, CPUs und Datenbanken zu überlasten, indem er auf Anmeldeseiten abzielt oder manipulierte Suchanfragen auf dynamischen Websites und Feedback-Seiten ausführt. Wenn die DDoS-Schutzlösung jedoch eine Deep Packet Inspection durchführt, können die Informationen genutzt werden, um den Datenverkehr mithilfe von maschinellem Lernen und künstlicher Intelligenz zu filtern.

Beispiele: GET, TLS, HTTP GET, HTTP Post

Netzwerkschicht (#3)

Ähnlich wie Transport Layer Floods zielen diese Angriffe darauf ab, die Bandbreiten- und Ratenbegrenzungsfunktionen der Firewall
zu überwältigen.

Beispiele: ICMP-Floods, IP-Fragmentierung, Verstärkungsangriffe (DNS, NTP, SSDP)

Transport Layer (#4)

Volumetrische Angriffe oder Floods verbrauchen Bandbreite und verlangsamen oder stoppen die Leistung des Webservers.

Beispiele: SYN-Flood, UDP-Flood, ACK-Flood, Angriffe zur Erschöpfung von Verbindungen (Sockstress, TCP)

7. MULTI-CLOUD-UNTERSTÜTZUNG

Unternehmen setzen zunehmend auf hybride IT-Landschaften, die aus eigenen Rechenzentren, Webservices und Anwendungen in privaten und öffentlichen Clouds bestehen. Um Risiken zu minimieren, sollten Unternehmen einheitliche Sicherheitsstandards für alle digitalen Arbeits- und Geschäftsumgebungen anstreben. Die unterschiedlichen DDoS-Schutzstandards in den verschiedenen Clouds können jedoch zu komplexen, verteilten Sicherheitsherausforderungen in Multi-Cloud-Konfigurationen führen. Dies führt häufig zu einem hohen Verwaltungsaufwand und uneinheitlichem Schutz, was letztlich die IT-Sicherheit schwächt. Umfassende DDoS-Schutzlösungen aus einer Hand sind eine effektive Möglichkeit, die Komplexität und die hohen Anforderungen an Verfügbarkeit und Leistung zu bewältigen. Der Einsatz von Schutzlösungen für alle genutzten Cloud-Plattformen ist eine bewährte Strategie.

Aus technischer, sicherheitstechnischer und Compliance-Perspektive gewährleistet dies einen konsistenten und zuverlässigen Schutz der gesamten IT-Umgebung des Unternehmens. Diese Lösungen sind für Cloud-Anbieter vorgesehen, auf das Unternehmen zugeschnitten und flexibel genug, um innerhalb der Cloud skaliert zu werden. Multinationale Unternehmen, die weltweit tätig sind, profitieren beim Schutz ihrer Infrastrukturen zudem von geringen Latenzzeiten.

8. COMPLIANCE

Bei der Absicherung digitaler Geschäftsprozesse müssen Unternehmen verschiedene nationale und internationale Vorschriften wie die DSGVO und das Bundesdatenschutzgesetz (BDSG) einhalten. Eine umfassende Lösung, die sowohl DDoS-Schutz als auch Rechtskonformität gewährleistet, ist daher unerlässlich. Herausforderungen ergeben sich oft, wenn die Schutzanbieter Serverstandorte außerhalb des GDPR-Rechtsraums der EU haben. Wenn ein Anbieter seine Dienste an Subunternehmer auslagert, kann dies die Transparenz, insbesondere im Hinblick auf die Einhaltung rechtlicher Anforderungen, erheblich beeinträchtigen.

Um die Daten- und IT-Sicherheit zu gewährleisten, sollten Unternehmen einen Anbieter mit Sitz in Deutschland oder Europa wählen, um das Risiko eines Datentransfers in die USA auszuschließen. Die europäischen und deutschen Gesetzgeber stellen strenge Datenschutz- und Sicherheitsanforderungen, die solide Schutzvorkehrungen bieten und die Einhaltung von Vorschriften vereinfachen. Um das Risiko noch weiter zu verringern, sollten Sie einen Anbieter wählen, der keine Niederlassungen in den USA hat, um einen möglichen Zugriff durch US-Einrichtungen zu vermeiden. Abgesehen von rechtlichen Erwägungen bieten Anbieter mit Sitz in der EU oft technologische Vorteile und haben ein tieferes Verständnis des europäischen Marktes und der Kundenbedürfnisse.

9. ÜBERWACHUNG UND VISUALISIERUNG

Ein webbasiertes Dashboard sollte umfassende Transparenz und Echtzeitüberwachung des Website- und Netzwerkverkehrs bieten.

Diese Dashboards bieten umfangreiche Funktionen, einschließlich der Möglichkeit, benutzerdefinierte Schutzparameter zu konfigurieren, den Datenverkehr in Echtzeit zu analysieren und Details über abgewehrte DDoS-Angriffe zu protokollieren.

Zu den wichtigsten Funktionen eines umfassenden Dashboards gehören:

- Detaillierte Berichte
- Konfiguration von Blacklists/Whitelists
- Einrichtung statischer Filterregeln
- Verwaltung global verteilter Schutzinfrastrukturen und verschiedener Schutzprofile
- Warnmeldungen
- Flexible Anpassungsmöglichkeiten

10. INTEGRIERTE PLATTFORM FÜR DDOS-BEZOGENE DIENSTE

Die Integration des DDoS-Schutzes mit anderen IT-Sicherheitslösungen gewährleistet einen umfassenden Leistungs- und Verfügbarkeitsschutz sowohl auf Netzwerk- als auch auf Anwendungsebene. Ein 360-Grad-Ansatz, der Tools wie Web Application Firewall oder sichere DNS-Dienste einbezieht, stärkt die Sicherheit zusätzlich. Eine vollständig integrierte Lösung von einem einzigen Anbieter beseitigt kritische Sicherheitslücken und bietet Vorteile wie:

- Koordinierte und miteinander verbundene Dienste
- Skalierbare Schutzfunktionen
- API-Integration für nahtlose Kompatibilität mit der bestehenden IT-Infrastruktur
- Geringerer Schulungs- und Verwaltungsaufwand

Die Entscheidung für eine einheitliche Plattform beseitigt Ineffizienzen und Kosten, die mit der Verwaltung mehrerer paralleler Lösungen verbunden sind, und strafft und stärkt die gesamte Sicherheitsstrategie.

11. SUPPORT UND MANAGED SERVICES

Umfassender DDoS-Schutz hängt von einem zuverlässigen, fachkundigen Support ab, der einen unterbrechungsfreien Betrieb gewährleistet. Wesentliche Support-Funktionen umfassen:

- **24/7-Verfügbarkeit:** Ein dediziertes Support-Team, das per E-Mail und Telefon erreichbar ist, um Vorfälle zu beheben, Fragen zu beantworten und andere Anforderungen zu erfüllen.
- **Proaktive Überwachung:** Ein SOC-Team, das den Zustand der Plattform überwacht, Anomalien und Vorfälle erkennt und sie umgehend behebt.
- **SLA:** Definierte Reaktionszeiten, die von Minuten bis Stunden reichen und in Service Level Agreements (SLAs) festgelegt sind.
- **Unterstützung beim Onboarding:** Expertenteams zur Erleichterung eines nahtlosen Onboardings, einschließlich Bereitstellung, Konfiguration und Integration mit SIEM/SOC und CI/CD-Pipelines.

FAZIT

Die Auswahl der richtigen DDoS-Schutzlösung ist eine wichtige Entscheidung, die sich direkt auf die Sicherheit, Widerstandsfähigkeit und Verfügbarkeit der IT-Infrastruktur Ihres Unternehmens auswirkt. Da DDoS-Angriffe immer ausgefeilter und umfangreicher werden, müssen Unternehmen Lösungen bevorzugen, die den aktuellen Sicherheitsanforderungen entsprechen und gleichzeitig an zukünftige Bedrohungen anpassbar sind.

In diesem Leitfaden werden die wichtigsten Funktionen und Kriterien erläutert, die zu berücksichtigen sind - von Skalierbarkeit und Automatisierung bis hin zu Multi-Cloud-Unterstützung und Compliance. Durch eine gründliche Evaluierung der individuellen Anforderungen Ihres Unternehmens - sei es Always-On-Schutz, hybride Bereitstellungsmodelle oder die Integration in umfassendere IT-Sicherheits-Frameworks - können Sie einen umfassenden Schutz vor DDoS-Angriffen gewährleisten.

Die Zusammenarbeit mit einem vertrauenswürdigen, erfahrenen Anbieter von DDoS-Schutz gibt Ihrem Unternehmen die Möglichkeit, sich auf das Kerngeschäft zu konzentrieren, ohne die Sicherheit oder Compliance zu gefährden. Die Investition in eine robuste, maßgeschneiderte Lösung schützt wichtige digitale Ressourcen, erhält das Vertrauen der Benutzer und verbessert die Widerstandsfähigkeit in einer sich ständig weiterentwickelnden Bedrohungslandschaft.

ÜBER LINK11

Link11 ist ein globaler Cloud-Sicherheitsanbieter, der Lösungen für Netzwerksicherheit, Anwendungs- und API-Schutz sowie Anwendungsperformance für eine Vielzahl von Branchen anbietet. Vom umfassenden Netzwerk-DDoS-Schutz bis hin zu einer fortschrittlichen WAAP-Lösung umfasst unsere Plattform eine Web Application Firewall (WAF), Web-DDoS-Schutz, Bot-Management (einschließlich ATO), API-Schutz und Secure CDN & DNS.

Die DDoS-Schutzlösung von Link11 schützt Unternehmen selbst vor den raffiniertesten Angriffen und bietet Zero-Time-to-Mitigate für bekannte Bedrohungen und Mitigation in weniger als 10 Sekunden für unbekannte Angriffsvektoren.

Get a Demo

LINK11

Link11 GmbH | Lindleystr. 12 | 60314 Frankfurt | www.link11.com