radware

Smart Network. **Smart** Business.

Was macht eine gute Anti-DDoS-Lösung aus? Die wichtigsten Auswahlkriterien im Überblick

Whitepaper

WHITEPAPER TEILEN

Table of Contents

Was macht eine gute Anti-DDoS-Lösung aus?

DDoS-Angriffe sind immer stärker auf dem Vormarsch. Viele Unternehmen werben mit einem „DDoS-Schutz“, doch welche Technologien Anwendung finden und welchen Schutz diese tatsächlich bieten, ist von Anbieter zu Anbieter ganz unterschiedlich. Bei der Auswahl eines Anti-DDoS-Anbieters sollten Sie deshalb die folgenden Fragen stellen, damit Sie den richtigen Partner für Ihr Unternehmen finden.

Umfang des DDoS-Schutzes

Wie umfangreich ist der angebotene DDoS-Schutz?

Die jüngsten Entwicklungen haben es gezeigt: DoS-Angriffe werden immer komplexer, dauern immer länger und nutzen oftmals gleich mehrere unterschiedliche Angriffswerkzeuge. Die Attacken richten sich gegen verschiedene Schwachpunkte der IT-Infrastruktur, wie die Netzwerk-, die Server- und die Anwendungsschicht. Volumetrische Flood-Angriffe wie UDP- oder ICMP-Floodings nehmen die Netzwerkschicht ins Visier. Ihr Ziel es ist, die Netzwerkressourcen des Opfers zu belegen bzw. derart zu überlasten, dass es letztlich nicht mehr erreichbar ist. Auf die Serverschicht zielen SYN-Floodings und so genannte „Low & Slow“-Angriffe, welche die Ressourcen des Servers auslasten sollen. Die Anwendungsschicht schließlich kann auf verschiedene Weise angegriffen werden, beispielsweise durch SSL-basierte Attacken, HTTP-GET- oder -POST-Floodings und den Missbrauch von Anwendungen. Eine gute Anti-DDoS-Lösung muss heute in der Lage sein, Angriffe gegen alle drei Schichten zu erkennen und abzuwehren.

Besteht Schutz vor SSL-basierten DDoS-Angriffen?

SSL-basierte DDoS-Angriffe richten sich gegen die gesicherten Online-Dienste des Opfers. Diese Angriffe sind einfach durchzuführen, aber schwer zu bekämpfen – das macht sie bei Angreifern so beliebt. Damit eine Anti-DDoS-Lösung SSL-basierte DDoS-Angriffe erkennen und abwehren kann, muss der Traffic zunächst mit den SSL-Schlüsseln des Kunden entschlüsselt werden. Das ist rechenintensiv und erfordert spezielle Hardware-Beschleuniger, damit die erforderliche Leistung aufgebracht werden kann. Da für die Entschlüsselung die SSL-Schlüssel des Kunden erforderlich sind, kann diese Aufgabe nicht außerhalb des Rechenzentrums des Kunden erfolgen, wie beispielsweise in der Cloud, sondern muss vor Ort durchgeführt werden.

Besteht Schutz vor DDoS-Angriffen auf Anwendungsebene?

DDoS-Attacken gegen Anwendungsressourcen werden immer häufiger und sind längst keine Seltenheit mehr. Sie richten sich nicht nur gegen das bekannte HTTP, sondern auch gegen andere durch DoS-Attacken angreifbare Anwendungsprotokolle wie HTTPS, DNS, SMTP, FTP oder VOIP. Zu den beliebtesten DDoS-Angriffen gegen die Anwendungsschicht gehören HTTP-GET- und HTTP-POST-Floodings, bei denen der Angreifer das Verhalten legitimer Benutzer nachstellt, die beispielsweise zum Herunterladen eines großen Bildes oder zum Ausfüllen eines Webformulars auf die Website zugreifen. Bei einem gut koordinierten HTTP-Flood-Angriff werden die Webserver des Opfers mit den Anfragen des Angreifers derart überlastet, dass Anfragen normaler Nutzer nicht mehr verarbeitet werden können. DDoS-Angriffe auf Anwendungsebene sind schwerer zu erkennen, weil der Netzwerk-Traffic nicht ungewöhnlich groß ist. Auch die Abwehr ist schwierig, weil jede einzelne Transaktion legitim zu sein scheint.

Besteht Schutz vor „Low & Slow“-DDoS-Angriffen?

Langsame DDoS-Angriffe mit geringer Leistung, so genannte „Low & Slow“-Angriffe, erzeugen langsamen Traffic in geringem Umfang und sind deshalb für normale Anti-DDoS-Lösungen kaum zu erkennen. Solche Angriffs-Tools nutzen üblicherweise eine Schwachstelle im HTTP-Protokoll aus, die es ihnen ermöglicht, Tausende von Verbindungen zu den Webservern zu öffnen, ohne diese wieder zu schließen.

Auf diese Weise werden alle verfügbaren Verbindungen des Webservers ausgelastet, so dass neue Anfragen nicht mehr bearbeitet werden können und der Dienst für legitime Nutzer unerreichbar wird: es kommt zum Denial of Service.

Abwehrtechnologien

Wie schützt die Lösung Ihr Unternehmen gegen volumetrische DDoS-Angriffe, deren Ziel eine komplette Überlastung Ihrer Internetanbindung ist?

DDoS-Attacken können auch in Form von volumetrischen Angriffen stattfinden, mit denen schlicht die komplette Internetanbindung des Opfers ausgelastet werden soll. Die Verteidigung gegen solche Angriffe kann nicht vor Ort stattfinden, sondern muss aus der Cloud erfolgen. Optimal ist eine Anti-DDoS-Hybridlösung, die den Angriff vom Unternehmen weg in die Cloud umleitet und gleichzeitig Informationen über den Angriff an die Abwehrmechanismen der Cloud weitergibt. Das gewährleistet eine reibungslose Übergabe an die Cloud und eine sofortige Abmilderung des Angriffs.

Wie unterscheidet die Lösung zwischen legitimen Benutzern und Angreifern?

Im Gegensatz zu sonstigen Cyber-Bedrohungen bestehen DDoS-Attacken aus einer Vielzahl legitimer Anfragen. Alleine die Menge zeitgleicher Anfragen stellt das Problem dar. Da jede einzelne Anfrage eines solchen DDoS-Angriffs legitim zu sein scheint, besteht die größte Herausforderung bei der DDoS-Abwehr darin, zwischen legitimen Anfragen einerseits und bösartigen Anfragen andererseits zu unterscheiden. Herkömmliche Anti-DDoS-Lösungen nutzen Schwellenwert-Methoden, bei denen Angriffe erkannt werden, sobald der Traffic einen vordefinierten Wert überschreitet. Dieser Ansatz liefert jedoch naturgemäß vergleichsweise viele falsch positive Ergebnisse und verhindert so den Zugriff legitimer Benutzer auf die Dienste. Neuere Anti-DDoS-Lösungen setzen auf ausgeklügeltere Abwehrmechanismen, wie beispielsweise eine Verhaltensanalyse. Dabei wird der aktuelle Traffic mit Normalwerten verglichen, und abhängig vom Ergebnis werden intelligente Entscheidungen zur Angriffsabwehr getroffen. Zusätzliche Mechanismen können verdächtige Quellen testen und anhand der Antwort feststellen, ob es sich um einen Bot oder einen legitimen Nutzer handelt.

Wie garantiert die Lösung legitimen Benutzern selbst im Falle eines Angriffs ein bestmögliches Benutzererlebnis?

DDoS-Attacken haben das Ziel, Online-Dienste für legitime Benutzer unerreichbar zu machen. Deshalb genügt es nicht, die Angriffe einfach nur abzuschwächen, sondern es muss sichergestellt sein, dass das Benutzererlebnis für legitime Besucher auch während länger andauernder DDoS-Angriffe möglichst gut ist. Optimal ist es, in der Abwehrlösung die für Anfragen der Angreifer zuständigen Hardware-Ressourcen von den Hardware-Ressourcen zu trennen, die sich um legitime Benutzeranfragen kümmern. Auch müssen die Ressourcen für legitime Benutzer immer verfügbar sein, selbst im Fall massiver DDoS-Attacken.

Wo im Netzwerk wird die DDoS-Abwehrlösung platziert? Werden andere Netzwerkelemente wie Firewall, IPS, ADC und WAF vor DDoS-Angriffen geschützt?

Die jüngsten DDoS-Angriffe haben es gezeigt: Herkömmliche Netzwerksicherheitslösungen wie Firewalls, IPS und WAFs können einen DDoS-Angriff nicht stoppen. Alle Opfer eines DDoS-Angriffs besaßen Firewalls und Intrusion-Prevention-Systeme (IPS) in ihrer Infrastruktur. Dennoch wurde ihre Verfügbarkeit derart beeinflusst, dass sie letztlich unerreichbar wurden. Firewalls, IPS, ADC- und WAF-Lösungen sind ganz ohne Zweifel unverzichtbar, aber sie sind schlicht nicht auf die neuesten DDoS-Entwicklungen ausgelegt und können im Fall eines DDoS-Angriffs selbst zum Nadelöhr werden. Der Radware 2012 Global Application & Network Security Report zeigte, dass bei rund 33 % aller DDoS-Angriffe die Firewall oder IPS-Systeme einen Engpass darstellen. Deshalb muss die DDoS-Abwehrlösung allen übrigen Netzwerkkomponenten vorgelagert sein, um diese im Fall eines DDoS-Angriffs schützen zu können.

Wie schnell erfolgt die Erkennung und Abwehr von Angriffen?

Die ideale DDoS-Abwehrlösung erkennt und blockiert Angriffe bereits an der Grenze des angegriffenen Rechenzentrums, noch bevor die IT-Infrastruktur beeinträchtigt wird. Ein so aufgestelltes Abwehrsystem erlaubt einen Schutz in Echtzeit. Rein cloud-basierte Lösungen ohne Detektoren im Rechenzentrum des Opfers schützen erst dann vor einem Angriff, wenn der Internet Service Provider (ISP) bösartigen Datenverkehr manuell an das Scrubbing-Center eines MSSP umleitet. Dieser Vorgang kann Minuten und im schlimmsten Fall sogar Stunden dauern, ist schwierig in der Handhabung und lässt das Opfer und seine Kunden im Fall eines DDoS-Angriffs im Grunde so lange völlig ungeschützt, bis der Angriff umgeleitet werden kann.

Die Berichterstellung

Versorgt die Lösung Sie im Fall eines Angriffs mit Informationen in Echtzeit?

SIEMs (Security Information and Event Managers) sind der zentrale Baustein, der Ihr Sicherheits-Team im Fall komplexer DDoS-Angriffe mit allen wichtigen Informationen versorgt. Aufgabe eines SIEM ist es, sicherheitsrelevante Vorfälle und Ereignisse, die mit einem DDoS-Angriff in Zusammenhang stehen können, zu erkennen, zu melden und zu Berichten zusammenzufassen. Hochentwickelte Anti-DDoS-Lösungen müssen eng mit SIEM-Systemen integriert sein, die in der Lage sind, Daten aus mehreren Quellen zu aggregieren, zu normalisieren und zu korrelieren. Neben einer automatisierten Informationserfassung und Risikobewertung sollten sie auch Echtzeitanalysen und –berichte sowie Protokolle, Angriffstrends und weitere Informationen bereitstellen, die das Sicherheitsteam bei der Verteidigung gegen den Angreifer unterstützen.

Erfahrung und Know-how

Stellt der Anbieter der gewählten Lösung auch ein 24/7-Notfallteam bereit, das Kunden im Fall eines DDoS-Angriffs unterstützt?

Selbst wenn Sie die optimale DDoS-Lösung gefunden haben und auf ein erfahrenes Team zählen können: DDoS-Angriffe können für jedes Unternehmen eine echte Herausforderung darstellen und unerwartet zu kritischen Situationen führen. Dauert ein DDoS-Angriff viele Tage lang oder kommen sogar völlig neue Angriffswerkzeuge und -methoden zum Einsatz, benötigen Sie neben der Anti-DDoS-Lösung auch ein Notfallteam aus Fachleuten, die tagtäglich mit DDoS-Angriffen konfrontiert sind und die Arbeit Ihres Sicherheitsteams unterstützen können.

Ist die gewählte Lösung markterprobt? Welche anderen Unternehmen setzen die Technologie ein? Nutzen auch führende Cloud-MSSPs, die Anti-DDoS-Dienste anbieten, die von Ihnen favorisierte Lösung?

MSSPs, die Anti-DDoS-Dienste bereitstellen, nutzen in ihren eigenen Rechenzentren zur Abwehr möglicher Angriffe Technologien und Produkte von Drittanbietern. Naturgemäß sind führende MSSPs beim Thema Anti-DDoS-Lösungen die anspruchsvollsten Kunden, weil sie um die Art möglicher Angriffe, die verschiedenen Abwehrmechanismen aber auch um die Erwartungen ihrer Kunden wissen. Fragen Sie deshalb nach Referenzkunden, die selbst schwerpunktmäßig Anti-DDoS-Lösungen anbieten.

Ist der Anbieter eine anerkannte Autorität auf dem Gebiet von DDoS-Angriffen?

Erkundigen Sie sich, ob der gewählte Anbieter seine Kompetenz belegen kann: durch Branchenauszeichnungen, Zertifizierungen, positive Rezensionen in den Medien und publizierbare Forschungsergebnisse zu den neuesten DDoS-Bedrohungen.