corero
FIRST LINE OF DEFENSE

ZUSAMMENFASSUNG

BRANCHE
Leistungsstarker regionaler Carrier mit zusätzlichen Mehrwert- und Netzdienstleistungsangeboten

HERAUSFORDERUNG
Automatisierte Abwehr von modernen DDoS-Angriffen, um Server-Ausfälle zu vermeiden und sich wieder 100 %-ig auf das Kerngeschäft konzentrieren zu können

LÖSUNG
Corero SmartWall® Threat Defense System (TDS)

RESULTATE
> Der Normalbetrieb kann jederzeit und zu 100 % aufrecht erhalten werden, ohne dass bestehende Systeme beeinflusst werden oder ständig Änderungen notwendig sind.

> htp ist mit einer Lösung in der Lage, sämtliche Transitverbindungen abzusichern und so auf komfortable Art und Weise die dahinter liegende Infrastruktur zu schützen.

> Wirksamer und für htp alternativloser Schutz vor modernen DDoS-Angriffen mittels In-Line-Methode; erkennen von DDoS-Angriffen, bevor sie einen kritischen Schwellenwert erreicht haben.

HAUPTVORTEILE
> Automatisierte Lösung erlaubt es htp sich auf das Kerngeschäft zu konzentrieren und nicht ständig auf die aufwändige DDoS-Abwehr mit freien Mitteln

> Wirksamer Schutz vor Application-Layer- und Multi-Vektorangriffen, auch vor solchen, die weniger als 5 Minuten dauern und nur wenig Bandbreite beanspruchen.

> Zusätzlicher Dienst, den der Carrier seinen Kunden anbieten kann, die zunehmend ihren Provider in die Pflicht nehmen, wenn es um die Abwehr von DDoS-Angriffen geht.

DIE DDOS-EVOLUTION. UND WARUM SIE GERADE PROVIDER BETRIFFT.

htp GmbH IN HANNOVER ENTSCHEIDET SICH FÜR DDOS-SCHUTZ VON CORERO NETWORK SECURITY

DER KUNDE

htp wurde 1996 in Hannover gegründet und gehört mit inzwischen über 200 Mitarbeitern zu den leistungsstärksten regionalen Carriern in Deutschland. Unter dem Motto „...htp Gut gewählt!“ konzentriert sich htp auf qualitativ hochwertige Angebote zu marktgerechten Preisen. Für die Kunden besonders vorteilhaft: alle Entscheidungsebenen der htp sind in Hannover konzentriert und somit bei Bedarf direkt erreichbar. Hinter htp stehen die Stadtwerke Hannover AG als Gesellschafter mit 50 % Anteilen und die EWE AG mit Sitz in Oldenburg, ebenfalls mit einer Beteiligung von 50 %. Zur Produktpalette des Unternehmens gehören Telefon- und DSL-Anschlüsse mit unterschiedlichen Bandbreiten, Mobilfunkangebote sowie Mehrwert- und Netzdienstleistungen. Dazu kommen skalierbare Daten- und Infrastrukturlösungen, die aus eigenen hochverfügbaren und hochsicheren Rechenzentren heraus angeboten werden. htp betreut über 9.600 Geschäftskunden und rund 88.800 Privatkunden in der Region Hannover, in Braunschweig und den Landkreisen Hildesheim, Peine und Wolfenbüttel.

DIE EVOLUTION VON DDOS-ANGRIFFEN UND DIE FOLGEN FÜR INTERNET SERVICE PROVIDER

Das World Wide Web hat in seinen 25 Jahren Lebenszeit zahllose Veränderungen durchgemacht. Das gilt gleichermaßen für die Versuche es zu manipulieren. Ein Beispiel dafür sind DDoS-Angriffe, die sich von rein volumetrischen Attacken zu trickreichen Täuschungsmanövern weiterentwickelt haben. Ein Großteil der aktuellen Angriffsformen hat mit den traditionellen volumetrischen Attacken nicht mehr allzu viel gemein. Die „neuen“ sind nicht nur ausgefeilter und trügerischer, sie treten auch häufiger auf. Mit traditionellen Gegenmaßnahmen ist ihnen nur unzureichend beizukommen. Ein Risiko für ISPs und Carrier. Gerade in jüngster Zeit haben DDoS-Attacken ein weiteres Mal ihr Gesicht verändert. Das gilt für alle Bereiche: Volumen und genutzte Bandbreite, die Art und Weise des Auftretens und die Häufigkeit. Parallel dazu haben sich die Netzwerke von Carriern und ISPs verändert: Die Netzwerke sind exponentiell gewachsen, die Zahl der Kunden ist immens gestiegen.

Ein ausgesprochen lukratives Ziel für DDoS-Angriffe also, bedenkt man die vielfältigen Möglichkeiten in ein System zu gelangen. Nicht zuletzt dient die aggregierte Bandbreite dazu DDoS-Angriffe mit einem hohen Schadenspotenzial ans Ziel zu bringen. Immer häufiger kommt es zudem vor, dass Endkunden an ihren Provider herantreten, weil sie mit Erpressungsversuchen unter Androhung von DDoS konfrontiert werden. Das war auch bei Kunden von htp der Fall. Die Kombination dieser Trends stellt neue Anforderungen an den Schutz vor DDoS-Angriffen als bisher, birgt aber auch Chancen. Es geht um zweierlei: eine Technologie, die genau auf das veränderte Anforderungsprofil zugeschnitten ist, und die effizienter arbeitet als die bisherigen Methoden. Und um die darin liegende Chance für ISPs, mit einem besseren Sicherheitskonzept neue Umsatzmöglichkeiten zu generieren.

DIE HERAUSFORDERUNG: Wissen, was vor sich geht

Zwar haben sich die Technologien mit den Jahren weiterentwickelt. Aber oft sind sie nur reaktiv und dadurch vergeht wertvolle Zeit. Sie sind nicht ganz billig und zu einem guten Teil nicht alleinig geeignet mit der Angriffsstruktur moderner DDoS-Angriffe und der mit ihnen einher gehenden Bedrohungen Schritt zu halten. Traditionelle Scrubbing-Center haben beispielsweise eine Achillesferse: Sie verlassen sich auf ein relativ grobes Beispielraster im Hinblick auf den Datenstrom. Auf dieser Basis „entscheiden“ sie, ob eine DDoS-Attacke vorliegt oder nicht. Das kann zu fatalen Fehleinschätzungen führen. Nicht selten ist es dann ein erfolgreicher Angriff, der dazu führt, sich intensiver mit dem Thema auseinanderzusetzen.

Robert Remenyi, verantwortlich für die Planung des Internet-Backbones bei der htp GmbH dazu: „Wir haben vor etwa zwei Jahren damit begonnen, die Peaks bei den Bandbreitenmessungen genauer anzusehen. Mit FlowAccounting haben wir die Möglichkeit die auffälligen Ausschläge zu analysieren. Die Untersuchung hat unsere Vermutungen bestätigt. Es hat tatsächlich DDoS-Angriffe gegeben und zwar in aller Regel UDP (User Datagram Protocol) Amplification Attacks. Einer der DDoS-Angriffsvektoren also, der öffentlich zugängliche Systeme wie schlecht konfigurierte DNS-Server oder Router und andere Schwachstellen ausnutzt.“

EVALUIERUNG

Allein durch die Aktivierung des FlowAccounting zeigte sich, dass es bereits DDoS-Angriffe gegeben hatte und zwar mehrheitlich UDP Amplification Attacks. Die erzeugten eine unmittelbare Gefahr für die htp-Infrastruktur. Das galt zum einen für Teile der zentralen Systeme aber es waren auch Leitungsengpässe zu befürchten.

„Da wir inzwischen täglich DDoS-Angriffe beobachteten, mussten wir schnell handeln. Wir haben als erste Maßnahme vergleichsweise einfache statische Filter auf existierenden Routern eingesetzt. Solche Filter sind so konzipiert, dass sie Angriffe verhindern oder stoppen, die bereits bekannt und eindeutig als solche identifiziert sind. Bei diesen Datenströmen ist erwiesen, dass es sich nicht um legitimen Traffic handeln kann. Das war für den Anfang eine durchaus wirksame Maßnahme. Allerdings reichen solche Lösungen nicht aus, wenn es sich um intelligente und neuartige Angriffsformen handelt. Wir haben parallel begonnen, uns nach Lösungen umzusehen, die diesem Angriffsprofil gerecht werden und an dieser Stelle unsere professionellen Ansprüche würden erfüllen können“, beschreibt Robert Remenyi die Situation bei htp.

Den letzten Ausschlag gab eine erfolgreiche Attacke, der es gelungen war ein zentrales System des Carriers zeitweise nicht verfügbar zu halten.

DIE LÖSUNG

Angreifer sind sich der Schwachstellen traditioneller Scrubbing-Center und anderer Methoden sehr bewusst und haben ihre Techniken dahingehend modifiziert. Mit einem niedrigeren Schwellenwert fliegen sie sozusagen unterhalb des Radars und verhindern so, dass der betreffende Traffic umgeleitet wird. Beispielraster wie sie in Scrubbing-Centern zugrunde gelegt werden, sind wenig geeignet die überwiegende Mehrzahl moderner DDoS-Angriffe zu identifizieren, geschweige denn adäquat darauf zu reagieren.

Heutzutage können DDoS-Angriffe deutlich mehr als „nur“ Dienste zu unterbrechen oder dafür sorgen, dass Webseiten nicht mehr erreichbar sind. Corero Network Security beobachtet seit gut einem Jahr eine stark steigende Zahl von kurzzeitigen DDoS-Angriffen, die nur wenig Bandbreite für sich beanspruchen. Angriffe dieser Art, die einen Dienst nicht unbedingt zum Erliegen bringen gewinnen neben den bekannten volumetrischen Angriffen zunehmend an Bedeutung. Der „DDoS Trends and Analysis Report“ von Mitte 2015 bescheinigt denn auch 95 % der erfassten DDoS-Angriffe eine Dauer von weniger als 30 Minuten. Etliche Attacken beanspruchen weniger als 1Gbps an Bandbreite und dauern weniger als 5 Minuten. Application Layer-Attacken und Multi-Vektor-Angriffe bestimmen dabei das Bild. Angesichts der veränderten Bedrohungslandschaft verlangen immer mehr Kunden eine bereinigte Pipeline, über die nur der erwünschte und bereinigte Datenstrom bei ihnen ankommt.

Man braucht also beides. Die unmittelbare Einschätzung, ob tatsächlich ein Sicherheitsvorfall vorliegt, genauso wie eine langfristige Analyse der Trends, um frühzeitig auf Entwicklungen reagieren zu können. „Unser Ziel war es mit Hilfe der neuen Technologie den Normalbetrieb von htp durchgängig aufrecht zu erhalten. Das System sollte im Hinblick auf die Prozesse bei htp so wenig Einfluss haben wie möglich und vor allem wollten wir nicht ständig Änderungen durchführen müssen. Jetzt schützen wir mit einer Lösung sämtliche Transit-Verbindungen und damit auf sehr komfortable Weise die gesamte dahinter liegende Infrastruktur."

Von der ersten Kontaktaufnahme mit verschiedenen Herstellern bis zur letztendlichen Aktivierung des Produktionssystems Anfang August 2016 ist etwa ein Jahr vergangen. Um sicher zu stellen, dass sich das Vorhaben in der gewünschten Art und Weise umsetzen lässt, folgte man dem im Projektmanagement üblichen Proof-of-Concept-Verfahren. Drei Hersteller schafften es in die entscheidende Phase: das marktführende Unternehmen, Corero Network Security und ein weiterer Wettbewerber, der mit einem sehr aggressiven Preis ins Rennen ging.

Aber die ausgewählten Lösungen unterschieden sich auch in technischer Hinsicht. Anbieter 1 nutzt eine Netflow-/Syslog- und BGP (Border Gateway Protocol)-Analyse. Die Mitigation besteht im Filtern der angegriffenen IP mittels Remote Triggerd BlackHoling (kurz RTBH) über eine Appliance. Dabei werden die Routingtabellen so konfiguriert, dass jeglicher Netzverkehr basierend auf seiner Ziel-IP-Adresse oder Absende-IP-Adresse (Source-based Remote Triggerd BlackHoling /SRTBH) nicht in das eigene Netzwerk geleitet, sondern „ins Nichts" umgeleitet wird. Wird dabei als Filter die Ziel-IP-Adresse verwendet, so wird der gesamte, an den Zielrechner gerichtete Datenstrom verworfen. Die Methode ist vergleichsweise leicht umzusetzen und mit geringem Konfigurationsaufwand verbunden. Sie wird aber genauso leicht zum Nachteil, weil durch das Filtern der angegriffenen IP mittels RTBH der Angriff sozusagen mit Unterstützung des Providers gelingt. Denn durch das Filtern des kompletten Datenverkehrs landet auch der erwünschte Datenstrom nicht mehr auf dem Server. Er ist also genauso wenig erreichbar als würde er weiterhin unter der eigentlichen Attacke stehen. Den zweiten Schritt, eine Ausleitung des verdächtigen Netzwerkverkehrs über ein Scrubbing Center, bewertete htp in diesem Fall als zu komplex. Corero Network Security und ein weiterer Mitbewerber verwenden demgegenüber die „In-Line"-Methode. Beim dritten Anbieter zeigten sich allerdings Schwächen bei den Einstellungen, was praktisch sofort zu falschen Positivanzeigen führte. Ein weiteres Manko: man konnte bei dieser Lösung nicht auf einen Monitor-Modus umschalten.

Noch einmal Robert Remenyi: „Die größte Herausforderung bei unserer Entscheidung waren tatsächlich die Kosten, denn die Systeme sind nicht ganz billig. Die Internetanbindungskosten an unsere Upstreams haben sich durch die Anti-DDoS-Lösung fast verdoppelt. Auf den ersten Blick „nur" um den normalen Betrieb aufrecht zu erhalten. Der personelle Aufwand hielt sich mit geschätzten ein bis zwei Monaten in Grenzen, und die Investitionskosten belaufen sich auf etwa 300.000 Euro. Trotzdem ist die Lösung für uns alternativlos, wenn es um einen wirksamen Schutz vor DDoS-Angriffen geht. Sie ist im laufenden Betrieb ausgesprochen einfach zu handhaben und die intuitive Benutzeroberfläche erleichtert das Handling zusätzlich. Wenn es komplizierter wird, können wir erfahrungsgemäß auf einen sehr verlässlichen und kompetenten Support seitens des Herstellers vertrauen.

Die Implementierung ist inzwischen fast vollständig abgeschlossen, und wir gehen davon aus, dass wir uns in Zukunft sehr viel besser auf unser Kerngeschäft konzentrieren können statt uns mit der DDoS-Abwehr zu beschäftigen. Es war eines unserer wichtigsten Ziele, den täglichen Aufwand bei der DDoS-Abwehr zu reduzieren und diese zu automatisieren. Dabei greifen wir auf die Erfahrung des Herstellers und dessen SoC zurück. Mit dem im Corero System mit enthaltenen Monitoring über Splunk waren wir schon vertraut und ohnehin sehr zufrieden."

CHANCEN UND RISIKEN FÜR PROVIDER

Dank moderner Hard- und Software ist es möglich auf moderne DDoS-Angriffe in Echtzeit zu reagieren. Dabei spielt die glockenförmige Verlaufskurve von DDoS-Angriffen eine gewichtige Rolle. Sie dient dazu, Detektoren, die Anomalien aufdecken sollen, in die Irre zu führen. Mit diesem in bestimmten Szenarien sehr erfolgreichen Modell spielen die Angriffe aber modernen Analyseplattformen in die Hand. Sie sind nämlich dahingehend optimiert eine DDoS-Attacke als solche zu erkennen, bevor sie einen kritischen Schwellenwert erreicht hat.

ISPs sind sich der Gefahr von DDoS-Angriffen zunehmend bewusster. Gleichzeitig steigt der Druck. Man kann sich leicht vorstellen was mit dem Ruf eines Service Providers passiert, wenn ein Kunde aufgrund einer DDoS-Attacke Datenverluste hat hinnehmen müssen oder eine Webseite nicht mehr zu erreichen war. Neben dem Risiko liegt hier aber auch eine große Chance für Provider, sich gegenüber ihren Kunden zu profilieren und vom Wettbewerb abzusetzen. ISPs sollten ihren Kunden eine dynamische Lösung zum Schutz vor DDoS-Angriffen anbieten, bei der diese nur für die tatsächlich genutzte Bandbreite im Falle einer Attacke zahlen und nicht für alle Eventualitäten. Über solche Angebote denkt auch htp bereits nach, denn sie sind für den Endkunden attraktiv.

FAZIT

Robert Remenyi zieht ein vorläufiges Fazit: „Für uns ist eine Lösung wie die gewählte tatsächlich alternativlos, und wir profitieren von den Vorteilen eines automatisierten, verteilten Ansatzes. Man kommt zwar mit den klassischen Methoden und freien Mitteln schon ziemlich weit, es bleibt aber ein gefährliches Restrisiko, dass weitere DDoS-Angriffe, vor allem neuere, eben nicht auf diese Weise gestoppt werden. Von den drei geschilderten Optionen haben wir die für uns am besten geeignete Variante ausgesucht. Der weitere Ausbau der Internet-Uplinks erfordert dann, dass wir diese auch über die Anti-DDoS-Appliances leiten. Und wir planen den Dienst in Zukunft unseren Kunden anzubieten. Denn Kunden nehmen ihren Provider zunehmend in die Pflicht, wenn es um den Schutz vor DDoS-Angriffen geht."

ÜBER CORERO NETWORK SECURITY

Corero Network Security ist der führende Anbieter leistungsstarker Lösungen, um DDoS-Attacken in Echtzeit abzuwehren. Service Provider, Hosting-Anbieter und Online-Firmen verlassen sich auf die mit vielen Industriepreisen ausgezeichnete Corero-Technologie. Corero schützt die Netzwerkumgebung vor DDoS-Angriffen durch eine automatisierte Angriffserkennung und -abwehr. Gleichzeitig enthalten sind Tools zur vollständigen Visualisierung des Netzwerkverkehrs, sowie Analyse- und Reportingtools. Die First Line of Defense® ist eine zukunftsorientierte Technologie gegen DDoS-Attacken in hochkomplexen Umgebungen mit einem sehr viel kosteneffizienteren Bereitstellungsmodell als bisher üblich. Weitere Informationen finden Sie unter www.corero.com

Corporate Headquarters
1 Cabot Road
Hudson, MA 01749 USA
Phone: +1.978.212.1500
Web: www.corero.com

Germany
Pappelallee 78-79
10437 Berlin
Germany
Tel. +49 30 609849 0514