Partnerschaft auf Augenhöhe: Warum man zur DDoS-Abwehr einen Spezialisten braucht

Cyberlink AG entscheidet sich bei DDoS-Abwehr für Lösung von Corero Network Security

Case Study

corero

Cyberlink

Case Study

Zusammenfassung

Branche

Managed Service Provider (MSP) für infrastrukturbasierte Dienste aus Telekommunikation und IT für Geschäftskunden; im Rahmen des „Bilanz Telekom Ratings“ wiederholt als einer der Top 3 Internet Service Provider in der Schweiz bewertet

Herausforderung

Gesamtumfängliche Lösung für das Anforderungsprofil eines ISPs zur Abwehr von DDoS-Angriffen, Service, der die komplette Infrastruktur schützt, ohne die Bandbreite zu beeinträchtigen, automatisierte DDoS-Abwehr in Echtzeit, genuine Inline-Lösung zur DDoS-Abwehr, kein zugekauftes Nebenprodukt

Lösung

Corero SmartWall Threat Defense System (TDS)

Ergebnis

DDoS-Schutz in Echtzeit, hochautomatisiert, mit extrem hoher Verfügbarkeit, ohne Beeinträchtigung der Basisdienste (Latenz, Bandbreite), schützt die gesamte Infrastruktur, die Cloud fungiert nur als Ergänzung

Vollständig transparente Lösung, bei höchstmöglicher Verfügbarkeit

Der Kunde

Cyberlink ist seit 1995 ein unabhängiger Schweizer Managed Service Provider (MSP) und konzentriert sich ausschließlich auf infrastrukturbasierte Dienste aus Telekommunikation und IT für Geschäftskunden. Cyberlink beschäftigt rund 30 engagierte Mitarbeiter in Zürich, welche tagtäglich ihr fundiertes Expertenwissen mit Leidenschaft für Technologie kombinieren und über 1.500 Geschäftskunden mit über 6.000 Anschlüssen in der ganzen Schweiz betreuen. Die Firma befindet sich zu 100 Prozent im Besitz des Managements. Cyberlink wurde 2015 im Rahmen des „Bilanz Telekom Ratings“ wiederholt als einer der Top 3 Internet Service Provider in der Schweiz bewertet.

Die Situation

Multi-Vektor-Angriffe und Adaptive DDoS-Angriffstechniken etablieren sich

Immer noch verbinden die meisten mit der Bezeichnung „DDoS“ automatisch Angriffe mit nur einem Angriffsvektor, nämlich dem volumetrischen. Solche Angriffe, die eine enorme Bandbreite verbrauchen, sind sehr viel leichter zu identifizieren und abzuwehren. In-house- oder Cloud-basierte Lösungen zur DDoS-Abwehr oder eine Kombination aus beiden sind probate Mittel. Analysen haben jedoch neben der steigenden Zahl von Brute-Force-Angriffen mit mehr als einem Angriffsvektor noch etwas anderes zu Tage gefördert. Hacker gehen demnach verstärkt dazu über adaptive Techniken

Ergebnisse weiter

Die Lösung wächst mit den Ansprüchen des Kunden und erlaubt zusätzlich die forensische Analyse bereits erfolgter Angriffe

Peering-Points bleiben unter der Hoheit des ISP wie gewünscht

Alle Kunden profitieren unmittelbar vom Schutz vor DDoS-Angriffe: Kunden, die gezielt angegriffen werden, profitieren bis zu einem Limit von diesem kostenlosen Service, zusätzliche Dienste inkludieren dann wichtige Logging-Details und die Möglichkeit Attacken forensisch zu analysieren

Speziell auf den Kunden zugeschnittenes, Usage-basiertes Finanzierungsmodell

cyberlink

einzusetzen, die es ihnen erlauben sich ein genaueres Bild von der jeweiligen Sicherheitsinfrastruktur zu machen. Mithilfe dieses Profils konzipieren sie dann eine maßgeschneiderte zweite und dritte Attacke, bei denen sie die Sicherheitsebenen genau dieses Unternehmens gezielt umgehen. Auch wenn volumetrische Angriffe weiterhin die häufigste Form einer DDoS-Attacke sind etablieren sich daneben gemischte und adaptive Angriffsformen.

Internet Service Provider in der Verantwortung

Mit der sich verändernden DDoS-Landschaft verändert sich nicht zuletzt die Rolle der Internet Service Provider. Sie werden von Firmen und privaten Kunden verstärkt in die Pflicht genommen, wenn es darum geht, nur einen bereits bereinigten Datenstrom weiterzuleiten beziehungsweise besseren DDoS-Schutz anzubieten. Wollen Provider nicht riskieren ihre Kundenbasis zu erodieren, müssen sie auf das veränderte Anforderungsprofil reagieren. Service Provider sitzen an einer Schlüsselposition, ganz einfach wegen der großen Bandbreite und der vielen angeschlossenen Endkunden. ISPs sind prädestiniert, unerwünschten, schädlichen Traffic bereits an vorgeschalteten Peering-Points herauszufiltern. Also bevor der komplette Datenstrom auf das Netzwerk des Kunden trifft.

Herausforderung und Anforderungsprofil

Im Zuge dieses veränderten Anforderungsprofils evaluierte Cyberlink zunächst einen Cloud-basierten Dienst. Hier hatte das Unternehmen bereits Erfahrungen gesammelt und in der Vergangenheit für einige Kunden derartige Modelle umgesetzt. Es stellte sich allerdings sehr schnell heraus, dass dies keine gesamtumfängliche Lösung für einen ISP sein konnte. Cyberlink suchte nach einem Service, der die komplette Infrastruktur schützt. Die Cloud sollte lediglich eine Ergänzung sein.

Eine für solche Fälle mittlerweile verfügbare Alternative zu Scrubbing-Centern sind In-Line-Lösungen, die in Echtzeit vor DDoS-Angriffen schützen. Provider können die Technologie an geeigneten Peering oder Transit Points installieren und skalieren. Solche Systeme haben den großen Vorteil, dass sie automatisiert arbeiten und so auf einen DDoS-Angriff in dem Moment reagieren, in dem er stattfindet. Das war es auch was Cyberlink suchte. Gleichzeitig sollte eine extrem hohe Verfügbarkeit gewährleistet sein, ohne die vom Provider

Vorteile

Hochspezialisierte Lösung, die alle Anforderungen eines ISPs mit der notwendigen Transparenz erfüllt und die zusätzlich kommerzielle Anreize bietet

Alle Kunden profitieren vom Schutz vor DDoS-Angriffen, in Echtzeit ohne jegliche Leistungseinbußen beispielsweise bei der Verfügbarkeit; Privatsphäre und Vertraulichkeit bleiben gewahrt, da die Daten nicht auf Servern im Ausland gehostet werden; das genügt den strengen Anforderungen an Datenschutz und Datensicherheit in der Schweiz

Wird den grundlegenden Veränderungen innerhalb der DDoS-Landschaft gerecht: Die Lösung liefert eine unmittelbare Einschätzung, ob tatsächlich ein Sicherheitsvorfall vorliegt, genauso wie eine langfristige Analyse der Trends, um frühzeitig auf Entwicklungen reagieren zu können

angebotenen Basisdienste in punkto Latenz oder Bandbreite zu beeinträchtigen.

Evaluierung

Eine komplett Cloud-basierte Lösung kam aus verschiedenen Gründen nicht in Frage. Zum einen gebe es in der Schweiz keinen geeigneten Anbieter. Der wäre aber nötig, um die hohen Datenschutzanforderungen zu erfüllen. Erst jüngst machte die in Anlehnung an Heartbleed „Cloudbleed“ genannte Sicherheitsschwachstelle von sich reden. Cloud-Anbieter sind zudem nicht in der Lage das komplette Anforderungsprofil eines ISPs abzubilden, da das Angebot eher für Unternehmen mit einer kleineren IP-Range und niedrigeren Bandbreiten ausgelegt sind. Ein Set-up für ISPs würde nicht nur viel zu komplex, sondern könnte neuere Anforderungen wie beispielsweise Amazon Web Services (AWS) nicht abbilden. Andere Anbieter von In-line-Lösungen hatten im Gegensatz zu Corero ihr Portfolio oftmals nur um eine zugekaufte Lösung erweitert. Dem Anforderungsprofil entsprach letzten Endes dann tatsächlich nur die Lösung von Corero Network Security.

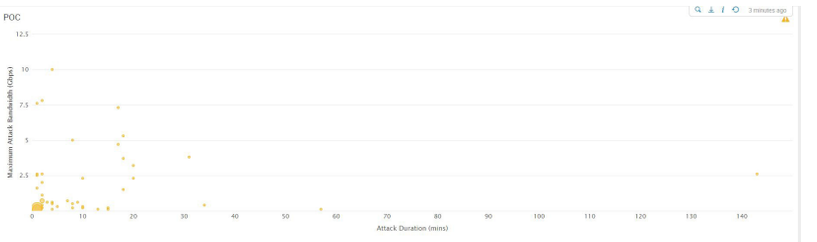
Die Lösung

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. 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.

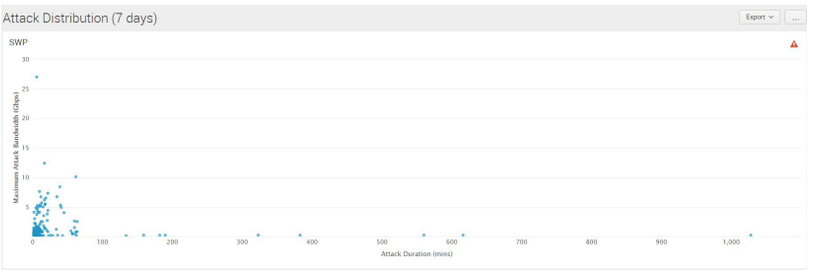
Sub-Saturating-DDoS-Angriffe – das smartere DDoS

Sicherlich werden wir zukünftig weitere Volumenangriffe sehen. Neu sind allerdings intelligente DDoS-Angriffe, die quasi „chirurgisch“ arbeiten: 84 % der beobachteten Angriffe dauern weniger als 10 Minuten, 71,6 % davon sogar nur

zwischen 0 und 5 Minuten, 93 % beanspruchen dabei weniger als 1Gbps und darunter . Dabei benutzten die Angreifer gerade genug Bandbreite um ihr Ziel zu erreichen. Traditionelle Lösungen zur Abwehr von DDoS-Angriffen übersehen solche Attacken. Selbst wenn sie auf dem Radar als Angriffe erkannt werden, sind sie oft schon vorbei, bevor man etwas gegen sie tun kann. Dabei folgen die Angriffe oftmals einem ganz typischen Verlauf über die Zeit. Und sie bleiben nicht folgenlos.



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.



Marc Chauvin, CTO der Cyberlink AG: „Mit Corero haben wir einen hochspezialisierten Anbieter gefunden, der alle Anforderungen eines ISPs erfüllt. Schutz vor DDoS-Angriffen ist die Kernkompetenz des Unternehmens und kein zugekauftes Nebenprodukt. Wir sind mit dieser Lösung nicht nur technisch ganz vorne mit dabei, sondern sie bietet uns und unseren Kunden auch eine Reihe von kommerziellen Vorteilen. Zudem ist es eine Partnerschaft auf Augenhöhe. Das spiegelt sich nicht zuletzt darin, dass der Hersteller für uns ein individuelles Finanzierungs- und Leistungsmodell ausgearbeitet hat.“

Guido Erroi, Regional Director bei Corero: “Die Rolle der Internet Service Provider beim Schutz vor DDoS-Angriffen hat sich bereits stark gewandelt. Qualitätsanbieter sehen sich in der Pflicht ihre Kunden vor solchen Angriffen zu schützen und zwar in Echtzeit. Für sie ist es untragbar, wenn durch eine DDoS-Attacke auf einen einzelnen Kunden gleichzeitig alle

anderen beeinträchtigt werden. Zudem suchen Provider nach Modellen, die sowohl technisch die nötige Transparenz bieten als auch kommerzielle Anreize. Die kommen beiden zugute, dem Provider und seinen Kunden."

Warum Corero: Die technischen Vorteile auf einen Blick

- Corero ist ein hochspezialisierten Anbieter für Lösungen zur Abwehr von DDoS-Angriffen (Kernkompetenz), kein zugekauftes Nebenprodukt
- DDoS-Schutz in Echtzeit, hochautomatisiert, mit extrem hoher Verfügbarkeit, ohne Beeinträchtigung der Basisdienste (Latenz, Bandbreite)
- Schützt die gesamte Infrastruktur, die Cloud fungiert nur als Ergänzung
- vollständige Transparenz
- skalierbar, die Lösung wächst mit
- forensische Analyse bereits erfolgter Angriffe
- always-on, höchstmögliche Verfügbarkeit von der ersten Sekunde an
- Peering-Points bleiben in der Hand des ISP, so dass ein größtmöglicher Grad an Freiheit erhalten bleibt, was sich naturgemäß nur mit einer lokalen Lösung realisieren lässt

Business Benefits für Cyberlink-Kunden

Coreo und Cyberlink sind sich einig: DDoS-Angriffe werden in Zukunft mehr und nicht weniger werden. Als Qualitätsanbieter sieht es Cyberlink als seine Aufgabe an Kunden entsprechend zu schützen. Marc Chauvin: „Es kann aus unserer Sicht einfach nicht sein, dass wenn ein Kunde angegriffen wird, alle anderen in Mitleidenschaft gezogen werden und offline gehen müssen."

- Sie profitieren von einem vollumfänglichen DDoS-Schutz in Echtzeit ohne jegliche Leistungseinbußen beispielsweise bei der Verfügbarkeit
- Privatsphäre und Vertraulichkeit bleiben gewahrt, da die Daten nicht auf Servern im Ausland gehostet werden; das genügt den strengen Anforderungen an Datenschutz und Datensicherheit in der Schweiz
- Alle Kunden profitieren vom Schutz vor DDoS-Attacken
- Kunden, die gezielt angegriffen werden, profitieren bis zu einem Limit von diesem kostenlosen Service, zusätzliche Dienste inkludieren dann wichtige Logging-Details und die Möglichkeit Attacken forensisch zu analysieren.

Fazit

Marc Chauvin abschließend: „DDoS-Angriffe haben sich in den letzten 10 Jahren fundamental gewandelt, das gilt sowohl für ihre Rolle als Vorbereiter von Ransomware- und Malware-Angriffen als auch für die spektakulären Volumenangriffe auf Basis von IoT-Botnetzen. Mit der Lösung von Corero Network Security sind wir für die veränderte Rolle eines ISP in punkto DDoS-Abwehr exzellent gerüstet, technisch wie kommerziell. In der Schweiz arbeiten wir mit unserem langjährigen Partner Boll Engineering zusammen. Boll und Corero haben gemeinsam ein speziell auf uns zugeschnittenes, Usage-basiertes Finanzierungsmodell ausgearbeitet mit dem wir rundherum zufrieden sind."

Über Corero Network Security

Corero Network Security ist führend in hochperformanten und in Echtzeit arbeitenden DDoS-Schutzlösungen. Internet-, Webhosting- und Onlineanbieter vertrauen auf Corero´s preisgekrönte Technologie, um DDoS Bedrohungen abzuwehren - mit automatischer Angriffserkennung und -abwehr, sowie mit vollständiger Netzwerk-Visibilität, Analyse und Reports. Diese nächste Technologie-Generation bildet eine erste Verteidigungslinie® gegen DDoS-Angriffe auch in den komplexesten Umgebungen, und bietet dabei noch günstigere wirtschaftliche Modelle als bisher verfügbar. Für weitere Informationen, siehe www.corero.com.

Corporate Headquarters
225 Cedar Hill St.
Suite 337
Malborough, Ma 01749 USA
Tel: +1 978 212 1500
Web: www.corero.com

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