Mehr Sicherheit und Verfügbarkeit für aixit-Kunden

Bewährter Schutz vor DDoS-Angriffen mit Arbor Peakflow und TMS

Kunde

aixit GmbH

Industriebranche

Internet-Service-Provider, Betreiber von Rechenzentren, Hosting-Provider

Die Aufgabe

Schutz der Infrastruktur des Rechenzentrums und der Kunden vor DDoS-Attacken mit einer Lösung ohne Online-Implementierung.

Die Lösung

DDoS- Bedrohungen und Attacken werden gezielt erkannt und abgewehrt. In einer Out-of-Band installierten Arbor Peakflow SP Lösung wurden die Arbor Peakflow SP Collector Platforms (CP) und Arbor Peakflow SP Threat Management Systems (TMS) für einen umfassenden Schutz kombiniert.

Das Ergebnis

Die Sicherheitslösung für aixit ist Out-of-Band installiert und behindert somit nicht den Kunden-Datenstrom. Die integrierte Peakflow SP- und TMS-Lösung erkennt DDoS-Angriffe und Bedrohungen frühzeitig und wehrt sie gezielt ab. Die Managed Security Services von Peakflow SP erschließen aixit neue Geschäftsfelder, verstärken die Kundenbeziehungen und tragen zu Kostenreduzierungen durch optimiertes Traffic Engineering bei.

Das Unternehmen

1996 in Aachen gegründet ist die aixit GmbH einer der ersten Internetpioniere in Deutschland. Heute ist das 2004 nach Frankfurt am Main umgesiedelte Unternehmen einer der führenden Anbieter für Managed Cloud Computing, Virtualisierung und Housing mit einem umfassenden Angebot an Rechenzentrums-, Hosting- und Internetdienstleistungen für Kunden in Deutschland und Europa. aixit verfügt über hochredundante Rechenzentren in Frankfurt am Main, Offenbach, Berlin, Hamburg und Amsterdam und besitzt ein eigenes europaweites Glasfasernetz mit zahlreichen Peering- und IP-Upstream Abkommen. Zu den derzeit über 250 Kunden gehören große Onlinespiele-Unternehmen, Sendeanstalten aber auch Privatkunden unterschiedlicher Größe in ganz Europa. Offizielle Partner von aixit sind unter anderem Versatel, Eunetworks, T-Systems, Colt Telecom und Dell.

Die Herausforderung: europaweiter Schutz vor DDoS-Attacken bei gleichbleibender Qualität und Verfügbarkeit der Datendienste

Durch die Nutzung gemeinsamer Rechenzentrumsdienste können Kunden Infrastrukturressourcen wie Server, ganze Räumlichkeiten und IT-Personal einsparen und ihre IT-Kosten reduzieren. Die Kunden lagern einen Teil Ihrer eigenen IT aus und nutzen bei aixit größere und moderne Strukturen mit zahlreichen Vorteilen. Dadurch erhöht sich jedoch für den einzelnen Kunden auch die Gefahr von DDoS-Angriffen (Distributed Denial of Services). In einer gemeinsam genutzten, geteilten Infrastruktur betrifft eine gezielte DDoS-Attacke auf einen bestimmten Kunden auch alle anderen Nutzer derselben Struktur.

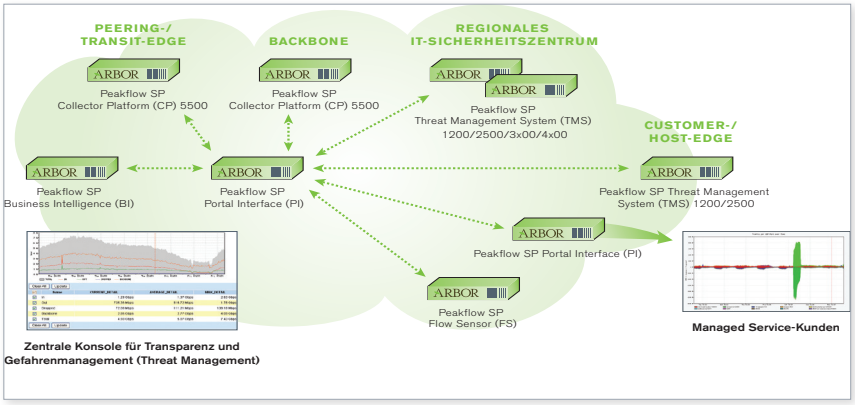
Die meisten Kunden verlassen sich beim Thema Sicherheit und Verfügbarkeit ihrer gehosteten Daten zunehmend auf den Betreiber des Rechenzentrums oder ihren Hosting-Anbieter. aixit sah sich in der Pflicht, dieser Anforderung gerecht zu werden und installierte schon 2010 entsprechende Schutzfunktionen, um DDoS-Attacken und daraus resultierenden Schaden für die Kunden abzuwehren. Holger Grauer, CTO bei aixit erklärt: „Die Häufigkeit von Angriffen hängt vom Kunden ab. Faktisch gab es für manche Kunden eine oder zwei Attacken pro Monat, während es für andere eine oder zwei pro Woche waren. Deshalb forderten vor allem große Kunden – darunter bekannte Sendeanstalten – einen optimierten, speziellen DDoS-Schutz. Kleinere Privatkunden waren an solchen Leistungen weniger interessiert, denn sie sind nicht oder nur selten das Ziel von Angriffen. Wir stehen aus unserer Sicht dennoch in der Pflicht, alle unsere Kunden gleichermaßen zu schützen.“

ARBOR® NETWORKS

Die Lösung: Gezielte Abwehr und Schutz des Rechenzentrums vor DDoS-Attacken mit Out-of-Band Konfiguration von Arbor Peakflow SP und TMS

Die IT-Profis von aixit machten sich auf die Suche nach geeigneten Lösungen für die optimierte Sicherheit ihrer Rechenzentren und der dauerhaften Integrität des Netzwerkes für alle Kunden. „Wir haben verschiedene Anbieter von Sicherheitslösungen recherchiert, und die Produkte von Arbor Networks haben uns am besten gefallen“, erklärt Grauer. „Einer der Hauptgründe, weshalb wir uns für die Arbor Peakflow SP- und Threat Management System (TMS)-Lösung entschieden haben, war der Vorteil, dass sie Out-of-Band verwendet werden kann. Die Lösung läuft parallel zu unserer Netzanbindung und erzeugt somit bei DDoS-Attacken keine Schwachstelle in der Verfügbarkeit unseres Netzwerkes.“

Das Sicherheitskonzept für aixit besteht in einer Kombination von Arbor Peakflow SP und der Peakflow Collector-Plattform (CP) mit dem Peakflow TMS, die wahlweise online oder Out-of-Band installiert werden kann. Peakflow SP CP ist eine Plattform für die netzwerkweite Absicherung der Infrastruktur und eine kosteneffiziente Überwachung des Datenverkehrs als Basis für die Sicherstellung der Verfügbarkeit. Es gilt heute als bewährter Sicherheitsstandard und wird von der Mehrzahl der weltweit führenden Internetdienstanbieter (ISPs) und international tätigen Unternehmen eingesetzt. Das ständig aktualisierte Produkt schützt mehr als 70 Prozent des globalen Internetverkehrs. Peakflow SP CP sammelt und analysiert die IP-Datenströme der Router des aixit-Netzwerks und liefert so eine umfassende Netzwerkeinsicht. Dadurch werden beispielsweise durch DDoS-Angriffe erzeugte Netzwerk-Anomalien aufgedeckt.



Kombiniert wurde Peakflow SP mit Peakflow TMS, das eine Angriffserkennung auch auf Applikationsebene ermöglicht und aktuelle Verhaltensmuster, so genannte „Fingerprints“, von bekannten und potenziellen Netzwerkbedrohungen bereitstellt. Solche Angriffe können in Folge erkannt und gezielt bekämpft werden, ohne den legitimen Geschäftsverkehr zu beeinträchtigen. Sowohl die legitimen Daten als auch die Angriffsdaten werden vom Border Gateway Protocol (BGP) zu den Peakflow SP TMS-Vorrichtungen umgeleitet. Der Angriff wird abgewehrt, während legitime Daten durchgelassen werden. Provider wie aixit können hierbei ihr Sicherheitsmanagement zusätzlich optimieren, indem sie aus den angebotenen Peakflow SP TMS-Vorrichtungen die für sie relevanten Modelle zur gezielten Abwehr von Angriffen auswählen. aixit setzt eine Kombination von TMS 2500 mit einer Bandbreite von 2,5 Gigabit pro Sekunde (Gbps) und TMS 3050 mit 5 Gbps ein.

Ergebnis: Umfassende Sicherheit, Kosteneffizienz und neue Dienste zur Stärkung von Kundenbeziehungen

aixit legt neben der Sicherheit und Verfügbarkeit seines Netzwerkes besonderen Wert auf seinen Kundendienst. Zuverlässigkeit, qualitativ hochwertige Leistungen und eine umfassende vertrauensvolle Betreuung stehen im Vordergrund. Schon wenige Monate nach der Implementierung der Arbor-Sicherheitslösungen bilanziert Grauer: „Die neuen Schutzleistungen überzeugen nicht nur technisch, sondern stärken auch nachhaltig unsere Kundenbeziehungen." Die Optionen zur Anpassung der Arbor-Produkte ermöglichen es, je nach Wunsch mehrere Ebenen von DDoS-Schutzleistungen (Bronze, Silber, Gold und Platin) anzubieten.

Der kombinierte Out-of-Band Einsatz von Arbor Peakflow SP und Peakflow TMS führte bei aixit zu folgenden Mehrwerten: Neben dem umfassenden Schutz der Rechenzentren und des Netzwerkes erschlossen sich neue umsatzfördernde Geschäftsfelder in Form von wertvollen Managed Services Angeboten für die Kunden. Außerdem optimierte aixit sein Traffic Engineering, was zu einer höheren betrieblichen Leistungsfähigkeit und Kostenreduzierungen führte. Zur optimalen Abwehr von DDoS-Angriffen wird aixit demnächst auch die von Arbor Networks in 2012 neu eingeführte Pravail-Produktreihe als zusätzlichen dedizierten Applikationsschutz im Rechenzentrum anbieten.

Pravail APS Web-GUI – „Summary"-Bildschirm. Durch Klicken auf die entsprechenden Symbole für „Protection Level" können vordefinierte Schutzmaßnahmen für einen Webserver oder andere spezifische Server/Gruppen in einem Rechenzentrum aktiviert werden.

„Wenn die Internetdienste unserer Kunden nicht funktionieren, wirkt sich dies auch auf unseren wirtschaftlichen Erfolg aus. Wir freuen uns daher, dass uns Arbor Networks bei der Abwehr von Angriffen und somit auch bei der Pflege unserer Kundenbeziehungen und unseren Geschäftszielen erfolgreich unterstützt."

Holger Grauer, CTO, aixit GmbH, Offenbach/Frankfurt am Main

Über Arbor Networks

Arbor Networks ist ein weltweit führender Anbieter von Lösungen für die Netzwerksicherheit und das Management von Next-Generation Rechenzentren und Carrier-Netzwerken. Die bewährten Lösungen von Arbor kommen weltweit in den Netzen von Internet Service Providern (ISPs) und großen Unternehmen zum Einsatz, sie fördern das Wachstum und stärken den Schutz von Kundennetzen, Unternehmen und Marken. Aufgrund der engen internationalen Geschäftsbeziehungen mit Service- und Hosting-Providern ist Arbor in der Lage, mithilfe von ATLAS (Arbor Threat Level Analysis System) fundierte Einblicke in die Internetsicherheit und Entwicklung des Datenverkehrs zu bieten. Durch die Zusammenarbeit von mehr als hundert Netzbetreibern auf der ganzen Welt ermöglicht ATLAS in Echtzeit den Austausch von Informationen über Sicherheit, Datenverkehr und Routing. Diese Informationen bilden die Grundlage von zahlreichen Geschäftsentscheidungen.

Weitere Informationen über Arbor Networks sowie Hinweise zu aktuellen Sicherheitsbedrohungen und Entwicklungen gibt es unter www.arbornetworks.com und im Sicherheits-Blog unter ddos.arbornetworks.com.

Arbor Network

Kontakt Deutschland/Schweiz
Arbor Networks
Michael Tullius
Territory Manager Deutschland/Schweiz

In der Au 40
60489 Frankfurt

Tel: + 49 69 78801656
Mobil: + 49 171 5439866
Fax: + 49 69 78801657
E-Mail: mtullius@arbor.net

www.arbornetworks.com