

16.01.09

Von: Tim Knudsen

Akamai: Sicher, schnell und kostengünstig - das Internet als internationale Geschäftsplattform



Teil 1: Grundlagen der sicheren und schnellen Bereitstellung von Anwendungen über das Internet - Angesichts der gegenwärtigen unsicheren Weltwirtschaftslage sind Kostenkontrolle und betriebliche Effizienz für IT-Strategien so wichtig wie nie zuvor. In dieser Situation müssen sich Unternehmen aller Art – von multinationalen Konzernen bis hin zu SaaS-Startups – verstärkt mit folgenden Fragen beschäftigen:

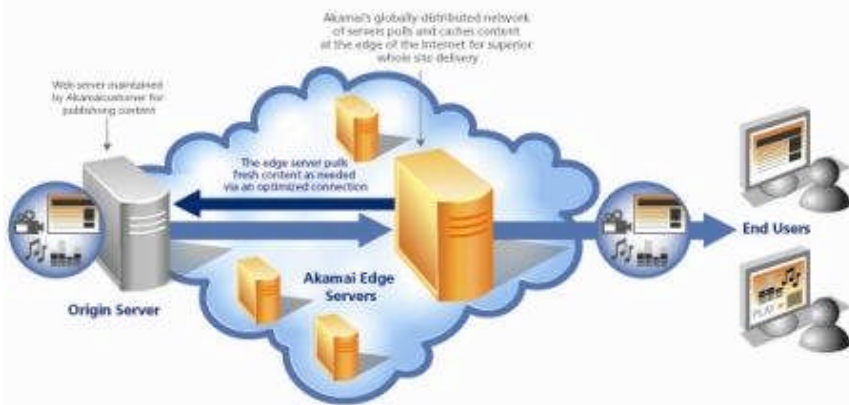
- Welche Infrastrukturen lassen sich zentralisieren und konsolidieren?
- Wie lässt sich mit den vorhandenen IT-Investitionen ein größtmöglicher ROI erzielen?
- Welche Geschäftsprozesse können über die Unternehmensgrenzen hinaus auf Partner und Kunden ausgeweitet werden, um die betriebliche Effizienz zu steigern?

Als Antwort auf diese drängenden Fragen verlagern immer mehr Unternehmen ihre Anwendungen in das Internet. Dabei dient das World Wide Web als Plattform für das Geschäftsnetzwerk, das ein Unternehmen mit seinen Kunden, Partnern und externen Mitarbeitern verbindet.

Diese Entwicklung wird in erster Linie von zwei Faktoren begünstigt:

1) Flexibilität: Das Internet ist äußerst flexibel. Die Vernetzung mit Kunden, Geschäftspartnern und Mitarbeitern kann unabhängig von privaten WANs erfolgen. Außerdem ist nahezu von jedem Ort auf der Welt aus ein Zugang zum öffentlichen Internet ohne Verzögerung gewährleistet.

2) Kosten: Mit der Verlagerung der Anwendungen ins Internet können Unternehmen die mit privaten WANs verbundenen IT-Kosten verringern, wenn nicht sogar vollständig vermeiden.



Bildupload

Trotz seiner grundsätzlichen Flexibilität und Kosteneffizienz ist das Internet jedoch per se keine sichere, hochverfügbare und performante Geschäftsplattform, weist es doch ganz klare Schwächen auf:

- **Mangelnde Perimeter-Sicherheit:** Das Internet kann unter Umständen mehr Risiken als Nutzen in sich bergen. Im Gegensatz zu privaten WANs existieren außerhalb des Rechenzentrums keine Kontrollpunkte oder Gateways. Die Firewall des Rechenzentrums kann somit zum Fokus gezielter Angriffe werden. Wie realistisch diese Gefahr ist, zeigen die Zahlen der jüngsten Berichte zum Internet-Zustand, in denen Akamai Technologies feststellte, dass die Zahl der Länder, von denen Attacken ausgehen, allein zwischen dem zweiten und dritten Quartal 2008 von 139 auf 179 anstieg.
- **Anfälligkeit von HTTPS- und VPN-Verbindungen:** Remote-Anwender, die HTTPS oder VPNs als Zugangsoptionen nutzen, sind den Unwägbarkeiten des Internet in Bezug auf Performance und Verfügbarkeit schutzlos ausgeliefert: Dazu gehören hohe und extrem schwankende Latenzzeiten bis hin zu Störungen in der Internetanbindung für ganze Regionen - wie sie bspw. im Februar und Dezember 2008 durch die Seekabeldurchtrennungen für Asien und den Mittleren Osten eingetreten sind - sowie die mangelnde Effizienz der TCP- und HTTP-Technologie. Dabei gilt: Je größer die Entfernung zwischen Anwender und Rechenzentrum, desto deutlicher wirken sich diese Unwägbarkeiten auf die Performance und Verfügbarkeit aus.
- **Fragmentierte Business Continuity-Lösungen:** Strategien für die Business Continuity werden auf Grundlage redundanter IT-Architekturen entwickelt, um so im Ernstfall den unterbrechungsfreien Betrieb sicherstellen zu können. Wird jedoch die Business Continuity außerhalb der Firewall, d.h. zwischen den Anwendern und den primären und Failover-Standorten, nicht berücksichtigt oder nicht gewährleistet, steht und fällt die Geschäftskontinuität mit der aktuellen Verfügbarkeit des Internet, auf der sie basiert.

Um diese Herausforderungen für Internetapplikationen zu meistern, muss bei der Anwendungsbereitstellung eine Strategie verfolgt werden, die innerhalb und außerhalb des Unternehmens Kostenreduzierungen und Effizienzsteigerungen ermöglicht, ohne dabei Sicherheit, Zuverlässigkeit und Performance zu beeinträchtigen.

Die Internet-Schwachstellen benötigen ein Kontrollsystem, das über die Firewall hinausgeht und sich auf die Middle Mile des Internet bis hin zum Endanwender erstreckt – und zwar unabhängig davon, wo sich dieser befindet. Möglich wird dies durch eine globale Infrastruktur, die auf dem Internet aufsetzt und so ein intelligentes Overlay-Netzwerk bildet. Dadurch entsteht eine virtuelle private WAN-Umgebung innerhalb des Internet, die eine sichere Verbindung mit Kunden, Partnern und Mitarbeitern ermöglicht und gleichzeitig für

ein Höchstmaß an Verfügbarkeit und Leistungsfähigkeit sorgt.

Die Wirksamkeit der Strategie eines globalen Overlay-Netzwerks wird maßgeblich durch die Verteilung und räumliche Nähe intelligenter Kontrollpunkte am Rande der Internetwolke bestimmt. Durch eine geringe Entfernung von lediglich einem „Network Hop“ zum Endanwender beziehungsweise zur Anwendungsinfrastruktur lässt sich eine binodale, symmetrische Kontrolle der Middle Mile erreichen. Dies bringt folgende Vorteile mit sich:

- Schaffung von Remote- und lokalen Perimeter-Firewalls innerhalb der Internetwolke, um so den Zugang zu Unternehmensinhalten zu kontrollieren und Internetattacken abwehren zu können.
- Intelligente Auswahl von Pfaden zwischen den Anwendern und dem Rechenzentrum zur Erzielung kürzester und konsistenter Latenzzeiten, um die Performance nachhaltig zu steigern.
- Intelligentes Routing des Datenverkehrs zwischen den Anwendern und dem Rechenzentrum, um Engpässe und Verfügbarkeitsprobleme im Internet zu umgehen und eine dauerhaft hohe Verfügbarkeit und Performance sicherzustellen, unabhängig vom aktuellen Zustand des Internets.
- Schwächen der Internet-Protokolle, die die Performance negativ beeinflussen, werden behoben, indem die standardmäßigen TCP- und HTTP-Protokolle so angepasst werden, dass die Anzahl der Roundtrips verringert und der Datendurchsatz maximiert wird. Die wiederholte Übertragung angeforderter Inhalte und Client-Antwortzeiten werden minimiert.



Bildupload

Dies ist der erste Teil einer insgesamt vierteiligen Artikelserie, die aufzeigt, wie Unternehmen das Internet als attraktive Lösung nutzen können, um ihre Infrastrukturkosten zu senken und die betriebliche Effizienz außerhalb der Firewall zu erhöhen ohne Zugeständnisse an Sicherheit, Zuverlässigkeit und Performance machen zu müssen. Dabei wird untersucht, wie sich eine redundante Perimeter-Sicherheit innerhalb der „Wolke“ des Internet herstellen lässt und wie VPN-Nutzern weltweit über das Web eine Umgebung ähnlich einem privaten WAN zur Verfügung gestellt werden kann, damit ohne Einbußen bei

Zuverlässigkeit und Performance und unabhängig von den jeweiligen Internetbedingungen eine verlässliche Business Continuity gewährleistet wird.

Tim Knudsen, Akamai Technologies



 www.akamai.de

- Verwandte Themen
- Akamai: Application Delivery – An Enhanced Internet Based Solution
- Akamai Technologies: Greifen Anwender aus großen Entfernungen auf die Applikation zu, kann sich die Antwortzeit verzehnfachen

Copyright All-About-Security.de / www.all-about-security.de Alle Rechte vorbehalten
Vervielfältigung nur mit Genehmigung von All-About-Security.de