

19.03.09

Von: Tim Knudsen

Erhöhen der Perimeter-Sicherheit durch eine effiziente Internet-Nutzung



Wie in Teil 1 bereits erläutert, zeigt diese insgesamt vierteilige Artikelserie auf, wie Unternehmen das Internet sinnvoll nutzen können, ohne Zugeständnisse an Sicherheit, Zuverlässigkeit und Performance machen zu müssen.

Teil 2 geht darauf ein, wie mit einer Cloud-basierten Internet-Infrastruktur mehr Sicherheit bei HTTPS-Anwendungen erzielt werden kann und somit eine redundante Perimeter-Sicherheit für Unternehmensapplikationen geschaffen wird.

Ende 2008 hat die Zahl der weltweiten Internetnutzer die 1,5 Milliarden-Marke überschritten. Seit Dezember 2007 sind geschätzte 61.940 Endnutzer-PCs täglich über den Internetzugang Bot-Attacken ausgesetzt. Da immer mehr Unternehmen ihre Anwendungen für Partner und Kunden über das Internet bereitstellen, steigt auch das unternehmerische Risiko durch immer neue Sicherheitsgefährdungen. Zu solchen Risiken gehören beispielsweise Hacker-Angriffe, Viren und Internetwürmer ebenso wie Denial of Service-Attacken oder das böswillige Verfälschen von Inhalten.

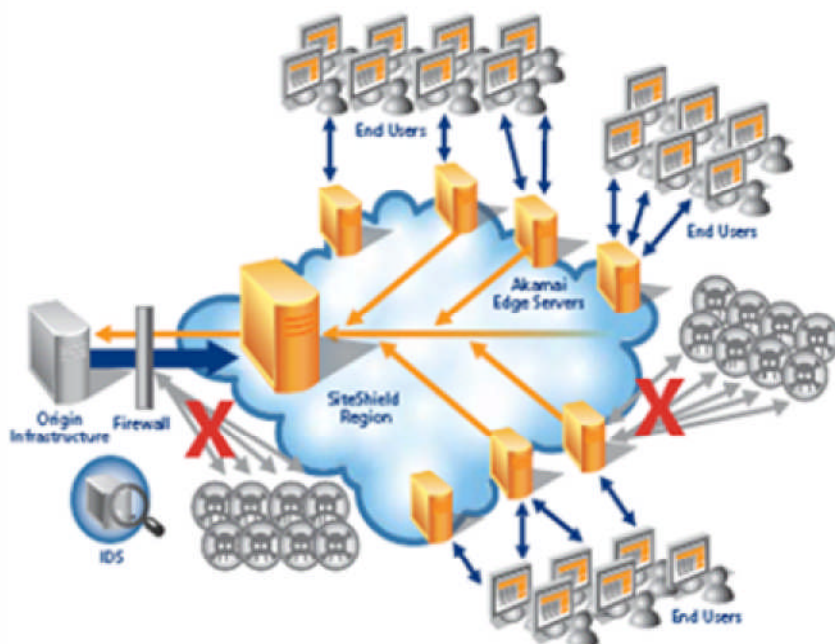
Unternehmenslösungen im Internet werden daher an der Sicherheit im privaten WAN gemessen. Dieses verfügt über zahlreiche Kontrollpunkte außerhalb des Rechenzentrums, mit denen sich ein mindestens zweistufiges Sicherheitskonzept realisieren lässt. So müssen sich die Nutzer zunächst im Netzwerk anmelden und erhalten erst nach einer weiteren Authentifizierung Zugriff auf die gewünschte Anwendung. Da Kunden und Geschäftspartner aber meist außerhalb des privaten WAN angesiedelt sind und nicht zum Unternehmen gehören, scheidet für diesen Anwenderkreis die Nutzung von VPN-Technologie aus geschäftlichen und technischen Gründen oftmals aus.

Dass die Erfüllung von Sicherheitsanforderungen bei der Bereitstellung von Webapplikationen außerhalb des WAN eine große Herausforderung darstellt, verdeutlichen zahlreiche Beispiele. Darunter fällt z.B. eine Supply Chain-Anwendung, auf die eine Vielzahl von wechselnden Sourcing-Partnern in Asien, Nord- und Südamerika zugreift. Ein zweites Beispiel ist ein globales Handelsportal für Hersteller aus dem Automobil- oder Schwermaschinensektor. Obwohl die Händler über ihre Geschäftsbeziehungen eng mit den Herstellern verflochten sind, handelt es sich um unabhängig agierende Unternehmen. Als drittes Beispiel kann die Trading-Plattform eines Finanzinstituts angeführt werden. Das Institut unterhält Geschäftsbeziehungen zu Händlern, wobei diese als Drittparteien auftreten. Um das Handelsvolumen steigern zu können, ist der Anbieter darauf angewiesen, neuen Händlern schnell einen gut funktionierenden Zugang zur Trading-Anwendung zu bieten.

Wie die obigen Beispiele zeigen, ist die Einbindung von externen Parteien aufgrund deren sich ständig verändernden Beziehungen zum Unternehmen über eine VPN-basierte Technologie äußerst schwierig. Aus technologischer Sicht kommt erschwerend dazu, dass VPN-Gateways erheblich mehr Kosten als Nutzen verursachen können, da zusätzlich zur Administration des Gateways auch bei den Anwendern Aufwand für Wartung und Support entsteht. Daher hat sich die Verschlüsselung über HTTPS-Verbindungen heutzutage breitflächig als Standard durchgesetzt. Diese Technologie bietet die nötige Flexibilität und hat sich im weiten Feld der Implementierungsmöglichkeiten auf breiter Front bewährt, wenn es um die sichere Bereitstellung von Unternehmensanwendungen geht.

Während die Vorteile von HTTPS-Verbindungen in der Zusammenarbeit mit Partnern und externen Mitarbeitern klar auf der Hand liegen, stellt sich die Frage, wie Unternehmen dabei ein hohes Maß an Kontrolle und Schutz, ähnlich einer VPN-Verbindung, erzielen können. Dies wird über eine Verlagerung der Kontrolle in die Internet-Wolke erreicht. Über einen solchen Edge Perimeter-Ansatz können Angriffe bereits abgefangen werden, noch bevor sie die Unternehmensinfrastruktur erreichen. So trägt dieses Vorgehen zu einer höheren Sicherheit bei.

- **Blockierung von „Malformed Requests“** : Da das Overlay-Netzwerk als Proxy für eine Anfrage dient, kann der vorgelagerte, intelligente Abwehrmechanismus diese Art von Anfragen und Datenpaketen bereits im Vorfeld abfangen, bevor sie die eigentliche Applikationsinfrastruktur erreichen.
- **Zugriffskontrolllisten**: Da die Anwender über das Overlay-Netzwerk eine Verbindung mit dem Firmennetz herstellen, können Zugriffskontrolllisten in den Edge-Bereich verschoben werden, um so den Zugriff einzelner Anwender zu gestatten bzw. zu unterbinden. Auf diese Weise wird innerhalb der Internet-Wolke eine Zugriffskontrolle auf VPN-Niveau erzielt.
- **Schutz des Ausgangsservers**: Der Applikationsserver befindet sich hinter dem Overlay-Netzwerk, das so einen wirksamen Schutz bietet. Der Zugriff auf die IP-Adresse des Servers von außen wird blockiert, nur der von einem nahegelegenen Edge-Kontrollpunkt des Overlay-Netzwerks stammende Traffic erreicht den Applikationsserver.
- **Schutz gegen DDOS-Attacken**: Da das Overlay-Netzwerk die Auslieferung von Inhalten und Daten für den Ausgangsserver übernimmt, kann es auch DDOS-bedingte Traffic-Spitzen abwehren und den Ausgangsserver vor Angriffen, die andernfalls durch ihre Tarnung als gewöhnliche Dateien oder Objekte als valide zugelassen werden, schützen.



Grafikupload

Teil 3 dieser Artikelserie befasst sich mit Business Continuity-Strategien, die auf dem Public Internet basieren. Das Public Internet ist ein „Netzwerk aus Netzwerken“, dessen Zuverlässigkeit nur allzu häufig überschätzt wird. Seine Verletzbarkeit zeigte sich erst kürzlich wieder bei einem Erdbeben in Taiwan und der Durchtrennung von Seekabeln in Nahost.

Wenn sich Business Continuity-Strategien auf das Internet stützen, ist eine Absicherung der darüber hergestellten Verbindungen gegen hohe Latenzzeiten und Datenverluste essenziell. Nur so kann eine echte Kontinuität gewährleistet werden - unabhängig davon, ob das Internet die Entfernung zwischen einem primären und einem Failover-Rechenzentrum oder zwischen Remote-Nutzern und einem oder mehreren Rechenzentren überbrückt.

Tim Knudsen, Akamai Technologies

 www.akamai.de

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