ANWENDUNGSFALL

Schnelle und sichere Bereitstellung von Unternehmensanwendungen

Zusammenfassung

Dank der digitalen Technologien entwickeln sich Unternehmen immer weiter. Damit verändern sich auch ganze Branchen. Mitarbeiter sind zunehmend mobil, und Geschwindigkeit und Effizienz sind heute unerlässlich. Deshalb benötigen Unternehmen dynamische, cloudbasierte Infrastrukturen sowie ungehinderten und sicheren Anwendungszugriff – überall, jederzeit und über jedes Gerät. Führende Anbieter müssen für ihre Weiterentwicklung Stolpersteine beseitigen, doch die hierfür erforderlichen Initiativen und Prozesse steigern die Angriffsfläche und gefährden so das Unternehmen.

Viele Organisationen greifen zu einem Zero-Trust-Sicherheitsmodell, um diese Herausforderungen zu bewältigen. Bei einer Zero-Trust-Architektur geht das System zunächst davon aus, dass das Netzwerk feindselig ist. Es wird nicht mehr zwischen innerhalb und außerhalb des Netzwerks unterschieden. Damit hat das Mantra „Vertrauen ist gut, Kontrolle ist besser" ausgedient. Stattdessen wird in entsprechenden Unternehmen nun ausschließlich auf Kontrolle gesetzt: Bei diesem Zero-Trust-Ansatz werden jedes Gerät und jeder Nutzer authentifiziert und autorisiert, bevor Anwendungen oder Daten bereitgestellt werden. Gleichzeitig werden Anwendungszugriff und Netzwerkaktivitäten über Protokollierung und Verhaltensanalyse überwacht.

Unter die vielen verschiedenen Anwendungsfälle für eine Zero-Trust-Sicherheitsstrategie fällt auch die schnelle und sichere Bereitstellung von Unternehmensanwendungen.

Schnelle und sichere Bereitstellung von Unternehmensanwendungen

Unternehmensnutzer sind zunehmend auf der Welt verteilt, und die Geschäftstätigkeiten finden nicht mehr nur in den vier Wänden des Büros statt. Mitarbeiter, Auftragnehmer, Partner, Zulieferer, Kunden und andere Mitglieder des Ökosystems von Unternehmen sind zunehmend mobil und verbinden sich remote mit dem Unternehmensnetzwerk – zu Hause, am Flughafen, bei Konferenzen, im Zug, im Hotel, im Café oder sogar in 10 km Höhe im Flugzeug. Unglaubliche 79 % der globalen Wissensarbeiter sind Telearbeiter[1] – eine Zahl, die seit 2005 um 115 % gestiegen ist. Und ein Ende dieses Trends ist laut IDC Research nicht in Sicht.[2]

Gleichzeitig sind auch die Unternehmensanwendungen zunehmend verteilt und müssen für geschäftskritische Vorgänge lokal und in der Cloud verfügbar sein. Und die Beliebtheit von Cloudanwendungen nimmt weiter zu. Im Durchschnitt nutzen Unternehmen mehr als 1.427 verschiedene Cloudservices – ein einzelner Arbeitnehmer nutzt täglich durchschnittlich 36 dieser Services.[3]

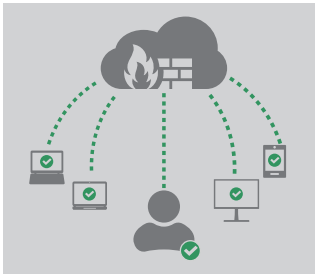
Um sich dieser neuen Situation anzupassen, setzen viele Unternehmen auf verschiedene Hard- und Software-Appliances, die gemeinsam den Netzwerkzugriff ermöglichen. Hierbei leiten sie den gesamten Cloudtraffic über einen zentralen Sicherheits-Stack in ihr WAN, nur um ihn dann über direkte Verbindungen oder VPNs zurück an die IaaS-Infrastruktur (Infrastructure as a Service) oder das Internet zu übertragen. Diese Ansätze sind allerdings weder aus betrieblicher noch aus finanzieller Sicht sinnvoll, zumal viele Unternehmen diese Stacks für verschiedene Regionen oder Cloudanbieter duplizieren müssen. Bei diesem Modell leiden Anwendungsperformance und Nutzererlebnis, während Unternehmensrisiken sowie Kosten und Aufwand steigen.

Durch Überlastung und Latenz verlieren Mitarbeiter, Partner und andere Nutzer wertvolle Zeit, weil sie warten müssen, bis wichtige Anwendungen geladen werden. Letztendlich bedeutet dies eine Verschwendung von Unternehmensressourcen (z. B. durch den Mehraufwand für Ihren IT-Helpdesk) und eine geringere Unternehmensproduktivität. Unternehmen leiten häufig Traffic zurück an das Unternehmensnetzwerk und verlassen sich bei der Verarbeitung auf komplizierte und aufwändige Konfigurationen – und öffnen damit Tür und Tor für Cyberangriffe auf ihre Infrastruktur und ihre Daten.

Darüber hinaus bieten entsprechende Frameworks oftmals keinen Schutz abseits des Netzwerks und ermöglichen die ungehinderte seitliche Verschiebung im Netzwerk, sodass jeder Nutzer freien Zugriff auf vertrauliche Informationen und Vorgänge hat. Solche komplizierten, aufwändigen und unzuverlässigen Strukturen treiben den Aufwand und die Kosten in die Höhe.

Werden Sie aktiv: Implementieren Sie Zero Trust

Die vorhandenen Techniken und Übertragungsmethoden sind einfach nicht mehr ausreichend. Die beste Lösung für einen schnellen, leistungsstarken und sicheren Zugriff auf Unternehmensanwendungen in heutigen hybriden Umgebungen besteht darin, die Unternehmensinfrastruktur über das Internet bereitzustellen und dabei proaktiv einen Ansatz zu verfolgen, bei dem niemals auf Vertrauen, sondern ausschließlich auf Kontrolle gesetzt wird. Diese Übertragungsmethode ist deutlich schneller, als den Traffic über das Unternehmensnetzwerk zu leiten. Und durch die Zero-Trust-Architektur werden jede Anfrage, jedes Gerät und jeder Nutzer authentifiziert und autorisiert, bevor Anwendungen oder Daten zur Verfügung gestellt werden. Da dieses Framework über die Cloud bereitgestellt wird und sich hinter einer Firewall befindet, sind Ihre IaaS-, SaaS- und Unternehmensinfrastruktur sowie Ihre Endpoint-Clients und IP-Adressen vor dem öffentlichen Internet verborgen.



Durch die Kombination von Cloudfunktionen, wie Routen- und Protokolloptimierung, mit Inhalts-Caching sowie der Integration von Identität, Single Sign-On (SSO) und Multi-Faktor-Authentifizierung (MFA) stellen globale Performance und Infrastrukturmanagement keine Herausforderung mehr dar. So können Unternehmen in allen Regionen und auch auf Mobilgeräten optimale geräteübergreifende Performance bieten.

Mit einem Zero-Trust-Sicherheitsmodell werden jede Anfrage, jedes Gerät und jeder Nutzer vor der Bereitstellung von Anwendungen oder Daten authentifiziert und autorisiert. Außerdem werden der Anwendungszugriff und die Netzwerkaktivität über Protokollierung und Verhaltensanalyse überwacht. So können Sie Unternehmensanwendungen in Ihrem gesamten Netzwerk schnell und sicher bereitstellen.

In „**Abschied von der klassischen Netzwerksicherheit**“ erfahren Sie mehr über das Zero-Trust-Sicherheitsmodell, und unter **akamai.com/eaa** finden Sie weitere Informationen zu den cloudbasierten, zentral verwalteten und einfach skalierbaren Akamai-Lösungen zur schnellen und sicheren Bereitstellung von Unternehmensanwendungen.

QUELLEN

1) Globale PGi-Umfrage zu Telearbeit, http://go.pgi.com/gen-genspec-15telesur-SC1129

2) IDC-Bericht zu Remotezugriff und Sicherheit, https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf

3) https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise/

Akamai

Als weltweit größte und renommierteste Plattform für die Cloudbereitstellung unterstützt Akamai seine Kunden dabei, ein optimales und sicheres digitales Erlebnis bereitzustellen – auf jedem Gerät, an jedem Ort und zu jeder Zeit. Die stark verteilte Plattform von Akamai weist mit über 200.000 Servern in 130 Ländern eine beispiellose Skalierbarkeit auf und bietet Kunden somit eine überragende Performance sowie einen umfassenden Bedrohungsschutz. Das Akamai-Portfolio für Website- und App-Performance, Cloudsicherheit sowie Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice und Rund-um-die-Uhr-Überwachung begleitet. Warum führende Finanzinstitute, E-Commerce-Unternehmen, Medien- und Unterhaltungsanbieter sowie Behörden auf Akamai vertrauen, erfahren Sie unter www.akamai.de, im Blog blogs.akamai.com/de oder auf Twitter unter @AkamaiDACH sowie @Akamai. Unsere globalen Standorte finden Sie unter www.akamai.de/locations. Veröffentlicht: April 2018