

Seriöse Angebote

Zertifizierte Managed Services für das Cloud Hosting

Fabian Kösters

Die Überlassung des Managements von IT-Infrastrukturen – sei es der Speicherplatz für die eigene Webseite oder ein Server – an Drittdienstleister ist im Hosting übliche Geschäftspraxis, insbesondere bei mittelständischen Unternehmen ohne eigene Server im Haus. Diese Vorgehensweise stellt aber auch einen großen Vertrauensbeweis gegenüber dem jeweiligen Anbieter dar. Zum einen werden damit wichtige Daten ausgelagert. Zum anderen steht und fällt mit der technischen Verfügbarkeit der Webseite oder des virtuellen Servers der wirtschaftliche Erfolg. Und das gilt nicht nur im E-Commerce. Auch Unternehmen anderer Branchen sind hier auf eine funktionierende IT-Infrastruktur angewiesen.

Webseiten sind ein Erfolgsfaktor. In den letzten Jahren sind sie immer komplexer, vielseitiger und multimedialer geworden. Wenn jedoch laststarke Webseiten, unternehmenskritische Anwendungen oder miteinander verknüpfte Webapplikationen zum Einsatz kommen, ist schnell eine hohe technische Komplexität der Serverinfrastruktur erreicht. In solchen Fällen ist klassisches Shared Webhosting wenig geeignet, den Anforderungen interner IT-Abteilungen an Verfügbarkeit, Flexibilität und Performance gerecht zu werden.

Es besteht nun die Möglichkeit, entweder eine eigene Infrastruktur im Unternehmen aufzubauen und sich um deren Unterhalt zu kümmern, oder diese als Co-Location in einem Rechenzentrum zu betreiben. Alternativ können Unternehmen auf Managed-Hosting-Lösungen zurückgreifen. Hier stellen Provider dem Kunden einen eigenen physischen Server zur Verfügung und übernehmen dessen Pflege und Administration.

Managed-Hosting-Lösungen können verschiedene Infrastrukturen zugrunde liegen: physische oder virtualisierte Infrastrukturen wie Cloud Infrastructure as a Service (IaaS). Und es ist auch möglich, verschiedene Infrastrukturstypen miteinander zu verbinden.

Cloud Hosting bedeutet Standardisierung

Managed Hosting ist eine von vielen Dienstleistungen, die auf Basis einer Cloud-basierten Infrastrukturebene geliefert wird, d.h., der Zugriff auf virtuelle Hardware wird bereitgestellt. Die Rechenleistung aus der Wolke ist hoch skalierbar und jederzeit verfügbar, während die Kosten für den Kunden sich lediglich nach den genutzten Ressourcen richten.

Anwendung findet das Cloud Hosting vor allem auch im E-Commerce. Die-

ser ist geprägt durch eine hohe Änderungsrate der System- und Anwendungsinfrastruktur, hervorgerufen z.B. durch immer wiederkehrende Lastspitzen. Die Webseite läuft nicht mehr auf einem physisch verortbaren Rackserver, sondern auf einem virtuellen Server, der auf einer Hardwareplattform installiert ist. In einer solchen Umgebung lassen sich variabel weitere, physisch bereits vorhandene Bauteile wie z.B. Prozessoren oder Arbeitsspeicher zu dem bereits installierten Server hinzuschalten.

Damit hat das Cloud Hosting vor allem dort seine Berechtigung, wo kurz-, mittel oder langfristig Lastspitzen auftreten können bzw. Ressourcen nicht genau planbar sind. Die redundanten Bauteile ermöglichen zudem einen Wartungskomfort, der bisher nur in Cluster-Systemen anzutreffen war. Hardwarekomponenten können ohne Serverausfall ausgetauscht werden, defekte Elemente werden augenblicklich erkannt und ersetzt.

Für alle Beteiligten erfolgreiches Cloud Hosting in Verbindung mit Managed Services bedeutet Standardisierung, denn Standardisierung heißt, dass Leistungen klar definiert und überprüfbar sind. Ein weiterer Vorteil liegt in der Einheitlichkeit der Systeme: Standardisierte Managed Hosting Server gewährleisten, dass Webanwendungen, die auf einem System laufen, dies auch auf allen anderen Systemen dieser Kategorie können. Hosting-Umgebungen bieten so eine verlässliche Plattform zum Betrieb von Webanwendungen, die mit geprüften Parametern in Bezug auf Nutzerzahl, Bandbreite und Anwendungssicherheit leistungsstark gehostet werden können.

Managed Services beim Cloud Hosting umfassen bei professionellen Webhostern das gesamte Server- und Betriebssystemmanagement, darunter die Verwaltung von Infrastruktursoftware auf der Middleware oder Persis-

Fabian Kösters ist Online-Redakteur bei Profihost in Hannover

tenzschicht, die Verwaltung von Webserversoftware, Anwendungs- und Datenbankserver, Verwaltung von Speichern inkl. Backup und Disaster-Recovery, Management der IT-Sicherheit, Verwaltung von Netzgeräten, Kapazitätsplanung, Performance-Tests und Rechenzentrumsmigration.

Service Level Agreement

Für Managed Server im Cloud Hosting sollten die zu erbringenden Dienstleistungen in einem Pflichtenheft, dem Service Level Agreement (SLA), vereinbart werden. Das stellt sicher, dass alle Vertragspartner von denselben Voraussetzungen ausgehen und effizient und verlässlich miteinander arbeiten können. Die Kriterien zur Festlegung eines Service Levels müssen messbar sein. Ein Service Level gilt als erfüllt, wenn genau festgelegte Schwellenwerte in einem definierten Zeitraum erreicht oder überschritten werden.

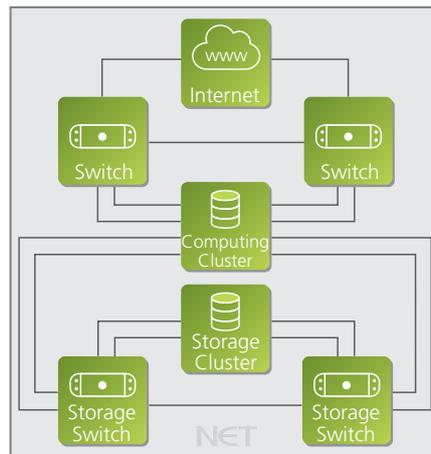
Im Service Level Agreement werden selbstverständlich Wartung und Pflege der Hardware übernommen. Dies beinhaltet Software- und Sicherheitsupdates, so dass nach Bekanntwerden von Sicherheitslücken, die immer wieder auftreten können, die entsprechenden Modifizierungen zeitnah zum Einsatz kommen. Die Server werden rund um die Uhr überwacht, und das Response-Team sollte ebenfalls 24 h am Tag erreichbar sein, um eventuelle Störungen direkt beheben zu können.

Managed Server Hosting bietet in den meisten Fällen eine Verfügbarkeit von 99,5 % bis zu 99,9 %. Dies bedeutet, dass die Server maximal 220 min/Jahr bis 44 min/Jahr nicht zur Verfügung stehen dürfen. Diese, wie auch alle anderen Merkmale sind im SLA definiert, z.B. Störungsklassen, Reaktionszeiten und das Prüfintervall der Server. Zusätzlich sollten SLAs über weitere optionale Features wie z.B. Prozessvisualisierung, DDoS-Schutzmaßnahmen und SSL-Zertifikate verfügen.

Zertifikate: Überprüfbarkeit von Leistungen

Wann immer von Cloud-Diensten gesprochen wird, geht es auch um die

Frage des Vertrauens in die Sicherheit. Eine neutrale Zertifizierung der Infrastruktur erhöht das Vertrauen in den Hosting-Anbieter. Vier Zertifikate können dazu als relevant angesehen werden. Es gibt aber noch zahlreiche weitere Prüfverfahren, die ein zusätzliches Maß an Sicherheit gewähren. Unternehmen, die Cloud-basierte Dienste beziehen, sollten sich vergewissern, ob zumindest eines dieser Zertifikate vorhanden ist:



Prinzip des Cloud Hosting

- ISO 27001 oder Trusted Cloud für infrastrukturbasierte Cloud-Dienste;
- EuroCloud SaaS Star Audit oder SAS-70 für SaaS-Angebote.

Internet Service Provider (ISP) sollten mit ihrem Hosting-Angebot für Managed Services eine hohe Betriebssicherheit und Verlässlichkeit ihres Dienstleistungsangebotes nicht nur versprechen, sondern sie auch belegen können. Da für Auftraggeber die Bewertung der Qualität der Managed Services eines Hosting-Anbieters im Voraus nahezu unmöglich ist, empfiehlt sich die Orientierung an unabhängigen Zertifizierungen. Externe Gutachter überprüfen, ob die in den SLAs definierten Vereinbarungen auch auf einem hohen Qualitätsstandard erbracht werden. Allerdings besteht für Hosting-Anbieter hierfür keine Verpflichtung, was dazu führt, dass viele von ihnen nicht einmal detaillierte Informationen darüber angeben, was unter ihren Managed Services konkret zu verstehen ist.

Die auf E-Commerce Hosting spezialisierte Profihost AG, ein mittelständischer ISP aus Hannover, lässt ihre Ma-

naged Services z.B. vom TÜV Saarland zertifizieren. Darüber hinaus gehend werden die Serversysteme im Cloud Hosting jährlich einem zertifizierten Penetrationstest zur Serversicherheit unterzogen. Diese stellen die IT-Sicherheit mit simulierten Angriffen auf die Systeme und IT-Infrastruktur auf die Probe mit dem Ziel, mögliche Schwachstellen zu erkennen und frühzeitig zu handeln. Hierbei werden – so auch bei Profihost – eine Hosting-Umgebung, das darunterliegende System, der SSH- und FTP-Zugang einer Hosting-Umgebung sowie die Login-Bereiche aus Sicht eines unangemeldeten Besuchers auf ihre Sicherheit hin überprüft. Dabei kommt ein Sicherheitsscanner zum Einsatz. Auch versuchen die Sicherheitsexperten manuell in das Testsystem einzugreifen.

ISO-27001-Zertifizierung

Diese Zertifizierung erfolgt, z.B. durch den TÜV, nach einem klar definierten Prüfschema. Im Wesentlichen geht es um die Erfüllung von Maßnahmen und Regelungen rund um die Datensicherheit. Im Fokus stehen dabei die 130 Kriterien der ISO-Norm 27001 des IT-Grundschutzes gemäß den Anforderungen des BSI und des Bundesdatenschutzgesetzes. Zentraler Bestandteil ist die Implementierung eines IT-Security-Managementsystems, das alle Maßnahmen und Verfahren, die vom Hostler eingesetzt werden, um ein vorgegebenes Sicherheitsniveau zu erreichen, enthält.

Überprüft werden die jeweiligen Leistungsbeschreibungen von Paketlösungen sowie von Einzelelementen. Dazu gehört auch die genaue Vorstellung und Erläuterung der relevanten dokumentierten Prozesse der Managed Services. Ein wesentlicher Prüfaspekt sind die angebotenen SLAs, in denen die Qualität der Leistungserbringung, Reaktionszeiten und die garantierte Verfügbarkeit geregelt sind sowie die Zuverlässigkeit von Datenschutz und -sicherheit. In Anlehnung an die ISO-Norm 27001 ist ebenfalls der Standort des Rechenzentrums in Deutschland ausschlaggebend und wird einer Untersuchung vor Ort unterzogen. Ziel dieser Maßnahmen ist es, dass diese relevanten gesetzlichen Normen zu

den Bereichen des Datenschutzes und der Datensicherheit ganzheitlich für das vom Hoster angebotene Dienstleistungspaket der Managed Services sichergestellt werden können.

Das erworbene Zertifikat weist einen hohen Standard der Managed Server beim Schutz vor unbefugtem Eindringen nach. Es gewährleistet ausgezeichnete Datensicherheit sowie die Einhaltung von Datenschutzbestimmungen nach deutschem Recht. Für Kunden bedeutet die Zertifizierung nach ISO 27001 eine hohe Verlässlichkeit in die Verfügbarkeit, Vertraulichkeit und Integrität sowie in die Sicherheit, sowohl sensible Daten als auch anspruchsvolle Technik in guten Händen zu wissen.

Trusted Cloud Service

Das Prüfverfahren Trusted Cloud der TÜV Trust IT prüft, basierend auf einem umfassenden Prüfkatalog, Cloud-basierte Dienste hinsichtlich organisatorischer und technischer Sicherheit, darunter Firewalls, Virenschutz und Verschlüsselung. Zusätzlich unterliegen die Compliance, z.B. hinsichtlich Datenschutz und Auditregelungen, sowie die SLAs und das Kapazitäts- und Backup-Management einer Überprüfung. Im Rahmen des Checks wird die Erfüllung der Kriterien aus dem Prüfkatalog mittels Interview und Dokumentenprüfungen abgefragt. Ein sich anschließender Prüfbericht enthält Empfehlungen der Prüfer, ob und unter welchen Voraussetzungen das Zertifikat erteilt werden darf.

EuroCloud SaaS Star Audit

Dieses Zertifikat wird vom Verband Eurocloud Deutschland – Eco e.V. ausgestellt. Der Verband hat mit dem Gütesiegel EuroCloud SaaS Star Audit ein Zertifikat speziell für Software-as-a-Service-Angebote (SaaS) eingeführt, das Dienste anhand ihrer Konformität mit Normen wie ISO 27001 und SAS-70 bewertet. Auch technische Sicherheitsmaßnahmen sowie die Einhaltung von gesetzlichen Vorgaben im Bereich des Datenschutzes werden überprüft. Im Einzelnen handelt es sich um die Überprüfung der Bereiche Datensicherheit und -schutz, Compli-

ance, Infrastruktur des Rechenzentrums, Anwendungsimplementierung sowie innerbetriebliche Prozesse. Eine Auditierung ist aufwendig, der Nutzer von SaaS-Angeboten hat allerdings die Sicherheit, dass der Cloud Service Provider strenge Sicherheits- und Qualitätsanforderungen erfüllt.

SAS-70

SAS-70, ausgestellt vom American Institute of Certified Public Accountants, gilt hierzulande in eingeschränktem Maß, ist allerdings insbesondere im angelsächsischen Raum von Bedeutung. Die Zertifizierung kann auf zwei Arten erfolgen, die sich vor allem in ihrem Umfang unterscheiden. Sie soll an dieser Stelle dennoch erwähnt werden, da insbesondere dann auf die SAS-70-Zertifizierung eines Cloud Service Providers zu achten ist, wenn IT-Services an ihn outgesourct werden, die mit dem Financial Reporting in Zusammenhang stehen. Der Prüfungsschwerpunkt liegt auf der Einhaltung der Vorgaben von Compliance-Regelungen wie Sox (Sarbanes Oxley Act).

Fazit

Cloud Hosting ist immer Vertrauenssache. Wichtige Daten werden ausgelagert und die Verfügbarkeit der Webseite in fremde Hände abgegeben. Unternehmen, die vor der Entscheidung stehen, ihre IT-Infrastruktur, ganz oder in Teilbereichen, an einen Cloud-Hosting-Dienstleister abzugeben, dienen Zertifikate als erstes Indiz für einen seriösen Anbieter. Dennoch sollten sie nicht blind auf vorhandene Zertifikate oder Gütesiegel vertrauen. Wichtig ist in diesem Zusammenhang auch zu überprüfen, wann diese ausgestellt wurden: Die meisten Zertifikate und Siegel müssen in regelmäßigen Abständen, häufig sogar jährlich, erneuert werden. Die Rezertifizierung geht immer auch mit einem neuerlichen Prüfverfahren einher, das vom Anbieter durchlaufen werden muss. In diesem Zusammenhang ist darauf zu achten, ob ganze Dienstleistungspakete oder nur Einzelelemente aus dem Hosting-Angebot zertifiziert wurden. (bk)