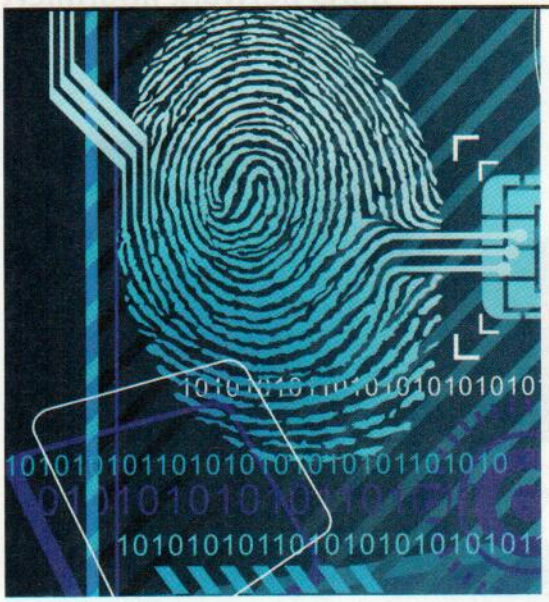


Bild: fotolia.com

Sicherer digitaler Geschäftsauftritt

Die Digitalisierung der Geschäfte bringt es mit sich: Unternehmen, Rechenzentrumsbetreiber und Internet-Dienstleister müssen die Art und Weise, wie sie ihre IT-Services bereitstellen und die daran beteiligten Daten schützen, völlig neu überdenken. Die Messlatte für beides liegt sehr hoch.

Autor: Hadi Stiel Redaktion: Markus Kien

Sind externe Clouds eine Alternative für sicherheitssensible Dienste und IT-Services? Nutzer könnten sich schon heute rundum sicher fühlen, meint Cloud World. Für das achtköpfige Team aus Marketing-, Business- und Cloud-Experten ist das Imageproblem externer Clouds, sie seien unsicher, gefährdeten Daten sowie Compliance und seien ein bevorzugtes Angriffsziel von Hackern, schon heute passé. Als Begründung für diese Behauptung führt Cloud World eine Studie von ReportsnReports ins Feld. Danach soll der Cloud-Software-Markt im Bereich Sicherheit in den nächsten vier Jahren um fast 50 Prozent wachsen. Je mehr Privatpersonen und Unternehmen Anwendungen und Daten in die Cloud verlagern würden, desto besser und flexibler würden die Sicherheitsvorkehrungen werden, versucht Frank Müller, Cloud-Experte und Gründer von Cloud World, die vermeintliche aktuelle Sicherheit externer Clouds mit einer mehr oder weniger wahrscheinlichen Marktentwicklung in den kommenden Jahren zu begründen. Cloud World hat als Marktplatz für Cloud-Produkte und -Dienste reges Interesse daran, dass Unternehmen vermehrt auf Cloud-Dienste setzen.

Auch die Analysten von Dynamic Markets, die im Auftrag von Cloud- und Rechenzentrums-Dienstleistern Marktbeobachtungen durchführen, sehen in der Studie „Managing Growth, Risk and the Cloud" für Unternehmen im Outsourcing von Daten, Anwendungen und Leistungen in eine Cloud nur Vorteile. Sie sollen durch das Auslagern im Schnitt ein Fünftel mehr an Zeit gewinnen, die sie für die Entwicklung von Innovationen nutzen könnten. Ebenso sollen 81 Prozent der Firmen vom Zugang zu einer hochentwickelten RZ-Infrastruktur profitieren, die sie sich aus eigenen Mitteln

funkschau EXPERTENKOMMENTAR

Bild: Materna

Ludger Wölfel,
Senior Consultant bei Materna

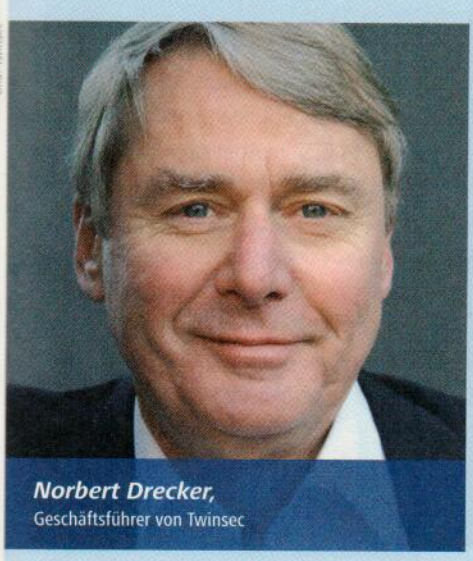
Multi-Provider-Management

Kaum eine IT-Organisation kommt mit einem Zulieferer für einen bestimmten Dienst aus. Mit der Anzahl der Dienstleister steigt jedoch nicht nur die Auswahl, sondern auch der Verwaltungsaufwand. Multi-Provider-Management ist angetreten, die Auswahl des jeweiligen Dienstleisters weitgehend zu automatisieren und damit sowohl die Nutzerzufriedenheit als auch die Servicequalität zu steigern.

Das Analysten- und Beratungshaus IDC sieht angesichts dieses Anforderungsprofils Unternehmen in die Rolle eines Service-Brokers hineinwachsen. Vor der Umsetzung eines professionellen Multi-Provider-Managements steht eine eingehende Recherche an, welcher Provider welche Leistungen zu welchen Kosten bietet, wie verlässlich und transparent SLAs und Charge-Back-Rückzahlungen von den einzelnen Anbietern gehandhabt werden und wer intern welche Leistungen abrufen darf. Die Hauptzielrichtung eines professionell herausgebildeten Multi-Provider-Managements sollte darin bestehen, im laufenden Betrieb sämtliche Leistungen permanent zu verfolgen, dazu die Administration dieser Leistungen weitgehend zu automatisieren. In gleicher Weise müssen die Überwachungsprozesse greifen, ob die von den Providern zugesicherten SLAs tatsächlich eingehalten werden. Treten SLA-beeinträchtigende Fehler auf, müssen diese selbsttätig dem zuständigen Provider zur Erstanalyse zugewiesen werden. Ebenso automatisch muss das Analyseergebnis ins Multi-Provider-Management-System des Unternehmens einfließen, um bei Bedarf via Portal Folgeaufträge für den zuständigen Provider generieren zu können.

Damit ein leistungsfähiges Multi-Provider-Management organisationsweit in Szene gesetzt werden kann, muss an weiteren Stellschrauben gedreht werden. Unverzichtbar sind ein Servicekatalog unter Berücksichtigung von Beschaffungsprozessen und Freigabestufen sowie eine umfassende Configuration-Management-Database (CMDB) einschließlich Asset-Management. Nicht fehlen sollte ein kompetenter Berater, der für das hochkomplexe Gesamtprojekt von Anfang an die richtigen Weichen stellt.

funkschau EXPERTENKOMMENTAR



Norbert Drecker,
Geschäftsführer von Twinsec

IT-Administration in hoher Qualität sicherstellen

Von der Qualität der IT-Administration hängt vieles ab: die Verfügbarkeit der zu erbringenden Services und der Geschäftsprozesse, die Qualität der Wartungsleistungen sowie das Niveau von Datenschutz und -sicherheit. Das gilt im Zusammenspiel mit Service-Providern für beide Seiten der Erfüllungskette. Umso wichtiger ist es, dies- und jenseits der Unternehmensgrenzen eine IT-Administration in hoher Qualität sicherzustellen.

Die Anforderungen an die Administration, auch auf Seiten der Provider, steigen mit dem Grad der Auslagerung. Je nach Spielart des Outsourcing speichert das Unternehmen selbst die Daten oder vertraut sie dem Provider an. Mit der ersten Auslagerungsstufe stellt der Provider lediglich die Infrastruktur bereit, inklusive neuer Patches und Versionen für die im Unternehmen installierte Software. Der Betrieb der Software und der damit verbundenen Schutz- und Sicherheitstechniken verbleibt im Unternehmen. Mit der zweiten Auslagerungsstufe gibt das Unternehmen den Betrieb und die Administration der Systeme, Anwendungen und Daten an den Provider ab. Mit der dritten Auslagerungsstufe delegiert es die komplette Service-Infrastruktur und die Betriebsverantwortung dafür an den Provider, genauer gesagt in dessen Cloud. Über sie werden mehrere Unternehmenskunden bedient. Mit der Betriebsverantwortung für die komplette Service-Infrastruktur legt das Unternehmen die Verantwortung für sämtliche administrativen Aufgaben in die Hände des Dienstleisters. Dazu zählen die Absicherung von Verfügbarkeiten mit entsprechenden SLAs sowie die Abschirmung der Daten innerhalb der Cloud durch Sicherheitstechniken wie VPN-Kanäle, Verschlüsselung, physische Zugangskontrolle, Prüfung logischer Berechtigungen und die Kontrolle, ob diese Berechtigungen über die Zeit eingehalten wurden.

Mit jeder Auslagerungsstufe mehr wächst also der Unternehmensanspruch an die SLAs und die Datenschutz- sowie -sicherheitsvorkehrungen des Providers. Und je mehr das Unternehmen die Kontrolle abgibt, umso mehr muss es sich darauf verlassen können, dass der externe An-. bieter seinen Kontrollaufgaben umfänglich nachkommt. Insbesondere der Kontrolle privilegierter User wie der Administratoren mit ihren erweiterten Zugriffsrechten für Systeme einschließlich der Management- und Sicherheitssysteme, Anwendungen und Daten kommt somit eine Schlüsselrolle zu. Nicht nur die Unternehmen, sondern auch die Provider werden marktreife Lösungen für das Management privilegierter User einsetzen müssen, um ihrer Rolle als qualitativ hochwertiger und vertrauensvoller Service-Dienstleister gerecht zu werden.

nicht leisten könnten. Weitere Vorteile laut Studie: Kostensenkung (71 Prozent), Entlastung des eigenen Personals (59 Prozent), höhere Stabilität und Verfügbarkeit der Services (58 Prozent) und bessere Skalierbarkeit (33 Prozent). Befragt wurden – kaum repräsentativ – 301 IT-Führungskräfte in Deutschland, Großbritannien und der Türkei. Die britische Dynamic Markets bezeichnet sich selbst als unabhängig, arbeitet aber als Research- und Consulting-Dienstleister nach eigenen Angaben für Größen wie Microsoft, Oracle und HSBC sowie Start-up-Unternehmen mit hohem Wachstumspotenzial.

Die Analysten sitzen als Marktförderer mit den Anbietern und Interessensgruppen oftmals in einem Boot. So werden Fragen für die Erhebungen so gestellt, dass die Antworten zu den erwünschten Ergebnissen führen. Für das Thema Outsourcing relevante Kriterien wie „drohender Kontrollverlust", „Kritikalität von Daten und Anwendungen", „Art der Services" und „Innovationsfähigkeit des Unternehmens" werden bei den Fragestellungen ausgespart. Ebenso ausgeblendet wird die steigende Gefahr für Unternehmen durch Wirtschaftsspionage, wenn sie geschäftskritische Daten und Anwendungen an Cloud-Dienstleister abgeben. Das gilt insbesondere für Cloud-Anbieter mit Hauptsitz in den USA und Großbritannien, die von den Geheimdiensten dieser Staaten offensichtlich mit mehr oder weniger Nachdruck zur Zusammenarbeit gezwungen werden.

Zwischen Kontrolle und Kontrollverlust

IT-Outsourcing ist und bleibt für Unternehmen ein Wagnis, auch wenn auf dem Etikett „Cloud" steht. Demzufolge hat sich an der generellen Leitlinie nichts geändert: Vertrauen ist gut, Kontrolle ist besser. Blindes Vertrauen geht in Zeiten der Ausspähungen gar nicht.

Gibt das Unternehmen Daten und Anwendungen an einen Cloud-Dienstleister ab, delegiert es die Kontrolle für diese Daten und Anwendungen. An die Stelle einer intern sowohl organisatorisch als auch technisch gut durchsetzbaren Kontrolle durch eigene Manager und durch eigenes Personal tritt eine externe Überwachung, die entfernt durch fremdes Personal ausgeübt wird und sich vorrangig an den geschäftlichen Vorgaben des Cloud-Dienstleisters orientiert. Wie verlässlich das Fremdpersonal Daten, Anwendungen und Systeme schützt, das kann ein Unternehmen lediglich mit Zeitverzug daran ablesen, ob vereinbarte Service-Level-Agreements (SLAs) für Sicherheitsdienste eingehalten wurden oder nicht – und das auch nur dann, wenn der Cloud-Dienstleister dem Unternehmen dafür alle notwendigen Informationen bereitstellt.

Zwar kann das Unternehmen gegenüber dem Cloud-Anbieter darauf bestehen, dass es periodisch sowie sporadisch Reports zu den auditierten Sicherheitsdienstleistungen abrufen darf, um auf diese Weise das Kontrollniveau anzuheben. Doch auch dieses Plus hat seinen Preis und ändert nichts daran, dass das Unternehmen nur mittelbar die Qualität der extern erbrachten Sicherheitskontrollen beeinflussen kann. Lückenlose Audits und Reports zu den Zugriffen und Prozessen speziell ihrer Administratoren stellen Cloud-Dienstleister erst gar nicht bereit, damit kein Zweifel an ihrer Verlässlichkeit aufkommt.

Dabei können besonders von diesen Administratoren aufgrund ihrer weitgehenden Berechtigungen, direkt wie indirekt, große Gefahren für die Daten und Anwendungen ausgehen.