zeptes weiter gedeihen. Die gute Nachricht dabei ist, dass es effektive Lösungen gibt, die IoT- und Industrie-4.0-Umgebungen wirkungsvoll schützen. Nun ist es an Unternehmen, diese vorausschauend zu implementieren. Wo es noch keine passenden Lösungen gibt, sollten Unternehmen kompensierende Maßnahmen treffen, wie zum Beispiel die Abschottung von kritischen Komponenten auf Netzebene. Ferner sollte die Entwicklung langfristiger Sicherheits- und Schnittstellenstandards weiter vorangetrieben werden, damit die Geräteherstellerin der Lage sind, Sicherheitsmechanismen zu implementieren, die herstellerübergreifend kompatibel sind. Erik Donner

2.2.2 Mit Cloud-Anbindung

Mit einer Box rein in die Cloud – und zurück

Wie hyperkonvergente Infrastruktur einem Rechenzentrum Cloud-Attribute verleiht und das Nutzen sowie Integrieren von Cloud-Services vereinfacht.

IT-Ressourcen müssen skalierbar und flexibel abrufbar sein. Compute- und Storage-Anwendungen sowie andere Services sollen sich einfach managen lassen – möglichst mit einem hohen Grad an Automatisierung im Betrieb. Die Public Cloud erfüllt diese Anforderungen, was Unternehmen dazu bewegt, Rechenleistung von extern zu beziehen und Anwendungen sowie Daten auszulagern. In der Regel entstehen so hybride IT-Landschaften, die Cloud-Services mit dem eigenen Rechenzentrum kombinieren, um letztendlich digital wettbewerbsfähig zu sein. Nur wer Innovationen schnell genug umsetzen kann, agiert künftig erfolgreich. Hyperkonvergente Infrastrukturen (HCI), deren zweite Generation gerade auf den Markt gekommen ist, schaffen im Rechenzentrum die Basis, um agil Produkte zu entwickeln.

Unternehmen, die HCI nutzen, können die Cloud-Vorteile ins eigene Haus holen. Diese Systeme wirken sich im Betrieb so positiv wie die Cloud aus und befähigen die eigene IT, schneller die benötigen Ressourcen bereitzustellen.

Merkmale hyperkonvergenter Systeme

Warum HCI 2.0 den IT-Betrieb effizienter macht, verrät ein Blick in Aufbau und Funktionsweise: Alle Komponenten – Server, Speicher, Netzwerk und Virtualisierungstechnik – sind in einer Box vereint. Die Hardware besteht aus mindestens zwei Chassis mit zwei Rechen- und vier Speicher-Nodes, die vom Speicherbetriebssystem und Hypervisor gesteuert werden. Applikationen steht ein Pool an virtualisierten Rechen- und Speicher-Ressourcen zur gemeinsamen Nutzung zur Verfügung. Typische Rechenzentrumsfunktionen wie Hochverfügbarkeit, Replikation, Datensicherung, Deduplizierung, Komprimierung oder WAN-Optimierung sowie Backup und Recovery sind integriert.

Eine wesentliche Stärke solch eines Mikrorechenzentrums ist eine garantierte Performance, auch bekannt als Quality of Service (QoS). Für jede Applikation wird ein Minimal-, Maximal- und Burstwert an IOPS festgelegt, wodurch der Betrieb aller Anwendungen störungsfrei läuft – auch im Parallelbetrieb auf einem System. Administratoren fügen je nach Bedarf neue Rechen- und Speicherknoten hinzu – unabhängig voneinander. Ein zentrales Dashboard vereinfacht das Managen der einzelnen Komponenten. Automatisierte Standardaufgaben wie Backups oder die Inbetriebnahme einer virtuellen Maschine (VM) reduzieren den Verwaltungsaufwand noch weiter.

Johannes Wagmüller, Director Solutions Engineering, NetApp

Integration in eine zentrale Datenmanagementplattform

Wenn die Anwendungen starten, müssen die Daten den Applikationen in dem Moment bereits zur Verfügung stehen. Der Verarbeitungsort, Cloud oder eigenes Rechenzentrum, darf da kein Hindernis darstellen. Das ortsunabhängige Datenmanagement setzt ein einheitliches Datenformat, eine einheitliche Datenübertragung und eine zentrale Datenmanagementplattform voraus. Diese Bedingungen erfüllt die NetApp HCI, die der Hersteller in sein Konzept der Data Fabric integriert hat. Ein Unternehmen ist dadurch in der Lage, Daten komfortabel zwischen verschiedenen Infrastrukturen und Speicherorten zu verschieben. In dem Fall unterstützen HCIs moderne Hybrid-Cloud- und Multi-Cloud-Umgebungen: Beispielsweise lassen sich die Daten für ein Disaster-Recovery-Szenario über hauseigene Schnittstellen direkt in die Cloud übertragen. Fallen Systeme im eigenen Rechenzentrum aus, wird einfach in der Cloud weitergearbeitet. Rechenleistung aus der Cloud zu beziehen, empfiehlt sich unter anderem für Business-Intelligence-Anwendungen, wenn diese nicht häufig laufen sollen. Lediglich die relevanten Daten werden für die Berechnung in die Cloud repliziert und die Ergebnisse abgeholt, wodurch sich Unternehmen die Hardware sparen. Wenn HCIs RESTful APIs intergiert haben, lässt sich auch ausschließlich Cloud-Computing im Sinne von Infrastructure as Code betreiben.

Zu den Cloud-Szenarien, für die sich HCIs besonders gut eignen, zählen Anwendungen für das Internet of Things (IoT). Gefragt ist in diesem

Umfeld ein System, das sowohl über Rechenleistung als auch Speicher verfügt und sich mit wenig Aufwand in Betrieb nehmen und managen lässt. Deshalb bietet es sich an, eine HCI im Maschinenpark als Mikrorechenzentrum zu installieren. Die Box analysiert Daten bereits am Entstehungsort, leitet nur relevante Informationen an das zentrale Rechenzentrum weiter – und überträgt bei Bedarf auch Daten in einen Cloud-Speicher.

Die Plattform, die wie die Cloud funktioniert

Unternehmen können HCIs für verschiedene Cloud-Szenarien als Plattform installieren, die für einen stabilen und effizienten IT-Betrieb sorgt. Durch das flexible und unabhängige Skalieren von Compute und Storage sowie der garantierten Performance lassen sich auf den hochintegrierten Systemen anspruchsvolle Geschäftsanwendungen im Rechenzentrum ohne großen Aufwand betreiben – wie in der Cloud. Das bedeutet: Die IT wächst oder schrumpft – je nachdem, welcher Bedarf besteht.

Johannes Wagmüller

Mit Cloud-Verschlüsselung Vertrauen schaffen

James LaPalme, VP Business Development & Cloud Solutions, WinMagic

Kaum ein Unternehmen in Deutschland kommt heute noch an der Cloud vorbei. Ob als Public-, Private- oder Hybrid-Modell oder in ihrer aktuellsten Form der hyperkonvergenten Infrastruktur, die virtuelle Wolke wird immer mehr zum Standard einer modernen IT-Umgebung. Doch um all ihre Vorteile wirklich sorgenlos nutzen zu können, müssen Unternehmen ihren eigenen Beitrag zur Sicherheit leisten. Der wichtigste Schritt dazu ist die umfangreiche Verschlüsselung aller Daten, die in der Cloud gespeichert sind.

Bereits KPMG und Bitkom konnten in ihrem Cloud Monitor 2017 die zunehmende Beliebtheit bei deutschen Unternehmen gegenüber der Technologie feststellen. Auch WinMagic hat Anfang 2018 in einer Studie den Trend bestätigen können: Demnach greifen 97 Prozent der IT-Verantwortlichen in der Bundesrepublik auf die Cloud zurück. Die Technologie ist mittlerweile klar etabliert. Allerdings sollte bei all der Euphorie der Sicherheitsaspekt nie aus den Augen verloren werden – insbesondere unter Berücksichtigung aktueller sowie neuer Anforderungen wie durch das IT-Sicherheitsgesetz oder die EU-Datenschutz-Grundverordnung (DSGVO).

Verantwortung in jeder Infrastruktur

Wer mit dem Auto nur ein paar Meter fährt, um den Parkplatz zu wechseln, muss dennoch den Sicherheitsgurt anlegen. Die Gurtpflicht gilt immer und überall – ob auf Landstraßen, in der Stadt, auf der Autobahn oder auf einer Spielstraße. Das gleiche Prinzip herrscht auch im Umgang mit (personenbezogenen) Daten. Denn es kommt nicht auf die Infrastruktur an, sondern stets darauf, ein möglichst hohes Sicherheitsniveau einzuhalten. Der Grund dafür: Die Verantwortung kann laut DSGVO nicht einfach auf jemand anderes übertragen werden.

Doch genau hier liegen einige Defizite: Spätestens mit Inkrafttreten der EU-Verordnung am 25. Mai können Unternehmen die Pflicht für die Sicherheit ihrer Daten nicht auf externe Dienstleister abwälzen. Allerdings geschieht genau das noch allzu häufig. So sehen sich nur 32 Prozent der Teilnehmer der WinMagic-Studie selbst in der Verantwortung, die Compliance ihrer Daten in der Cloud sicherzustellen. Demzufolge gehen mehr als zwei Drittel ein unnötig hohes Risiko ein. Denn kommt es zu einem Datenleck beim Cloud-Anbieter und der Cloud-Kunde ist nicht in der Lage zu beweisen, die eigenen dort gespeicherten Daten selbst geschützt zu haben, können hohe Strafzahlungen von bis zu 20 Millionen Euro verhängt werden.

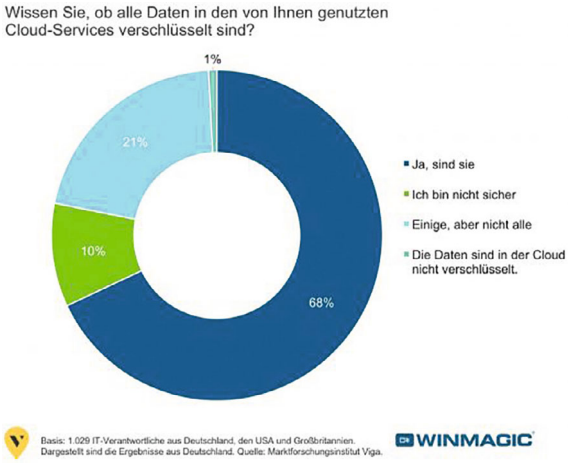
Verschlüsselt hält besser

Dass die Gefahr eines Datenlecks keineswegs gering einzuschätzen ist, haben im vergangenen Jahr hinreichend viele Fälle klar vor Augen geführt: Genannt seien hier lediglich Yahoo (rund drei Milliarden Accounts), Equifax (127 Millionen Datensätze) und Uber (57 Millionen Datensätze). Auch wenn die drei Beispiele sich in ihrer Intensität und den Ursachen unterscheiden, so zeigen sie ganz deutlich die Gefahr, denen Daten immerwährend ausgesetzt sind. Gleichzeitig hätte eine seit mehr als 20 Jahren etablierte Technologie in der IT ein paar Sorgenfalten vermeiden können: die Verschlüsselung.

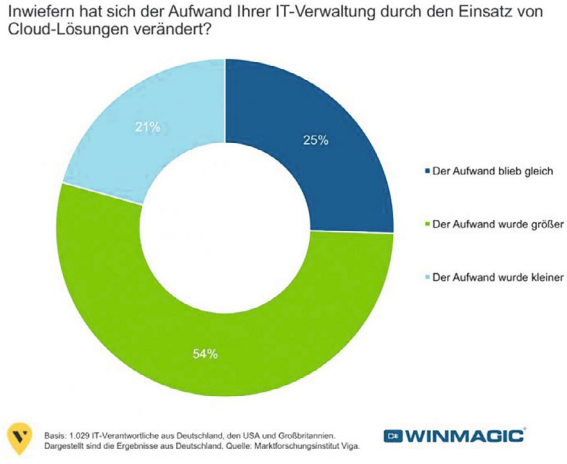
Ein modernes Cyber-Security-Konzept besteht aus einer ganzen Reihe von präventiven, proaktiven und reaktiven Maßnahmen. Darunter fallen etwa Virenscanner, Antimalware-Programme, Firewalls, VPN-Netzwerke oder die Zwei-Faktor-Authentifizierung. Doch wenn alle Stricke reißen und Daten entweder absichtlich entwendet oder versehentlich in die falschen Hände geraten, dann ist die Verschlüsselung die letzte und stärkste Verteidigungslinie. Das gilt nicht nur für lokal, sondern ebenso für die Cloud und die neusten hyperkonvergenten Infrastrukturen. Und dabei reicht es nicht aus, dass der externe Anbieter Verschlüsselung einsetzt. Jedes Unternehmen muss selbst die eigenen Daten in Cloud-Umgebungen schützen. Denn verschlüsselte Daten können von anderen nicht gelesen werden und gelten der DSGVO zufolge auch nicht als wirklich verloren.

Den Überblick behalten, Kontrolle garantieren
Eine gewisse Sorglosigkeit und Nachholbedarf beim Umgang mit Daten in der Cloud zeigte sich auch bei der WinMagic-Umfrage. Die befragten deutschen Unternehmen stehen demzufolge vor gleich zwei Problemen:

- Erstens können nicht alle mit Gewissheit sagen, ob ihre Daten in der Cloud verschlüsselt sind: Nur zwei Drittel der Teilnehmer (68 Prozent) sind sich sicher, dass ihre Daten vom Cloud-Service-Provider verschlüsselt werden. 21 Prozent verschlüsseln die Daten nur teilweise. Zehn Prozent der Befragten wissen nicht einmal, ob und wie ihre Daten verschlüsselt sind, und ein Prozent gibt sogar an, überhaupt keine Verschlüsselung einzusetzen.



- Das zweite Problem: Die IT-Verwaltung ist durch den Einsatz von Cloud-Lösungen komplizierter geworden. Dies gab mehr als die Hälfte der Teilnehmer (54 Prozent) an.



Dabei ist ein sicherer und einfacher Umgang mit Cloud-Umgebungen möglich, bei dem sowohl die Übersicht beibehalten als auch die rechtlich relevanten Compliance-Vorschriften eingehalten werden können.

Nötig ist dazu eine intelligente Management-Lösung, mit deren Hilfe die Verschlüsselung der Daten, die Verwaltung von Verschlüsselungs-Keys, Berechtigungen und Zugängen ebenso wie die ganzer Infrastrukturen und deren Bootvorgang zentral steuerbar ist. Zudem sollte die Kontrolle gleichzeitig nicht nur über verschiedene Cloud-Instanzen – darunter ebenso VMs – und lokale Umgebungen möglich sein, sondern auch die aktuell neuen hyperkonvergenten Infrastrukturen miteinschließen. Letztere werden immer beliebter, da sie Unternehmen im eigenen Rechenzentrum eine der Cloud ähnliche Performance bei Leistung und Skalierbarkeit bieten. Daher sollte ein intelligentes Key-Management, über das etwa WinMagics SecureDoc CloudVM verfügt, in der Lage sein, auch die VM-Architektur einer hyperkonvergenten Infrastruktur zu berücksichtigen.

Kundendaten in sicheren Händen
Mit der DSGVO wird ein Teil des Verbraucherschutzes an die aktuellen Gegebenheiten der Digitalisierung angepasst. Personenbezogene Daten treten heute fast überall auf und Kunden müssen darauf vertrauen, dass Unternehmen diese sorgfältig und hochsensibel behandeln und dabei nie den Überblick verlieren. Das gilt besonders, wenn IT-Infrastrukturen von Organisationen sich aus mehreren, ganz unterschiedlichen Modellen zusammensetzen. Maßnahmen wie ein lückenloses Monitoring und die zentrale Steuerung der Vergabe sowie des Löschens von Verschlüsselungs-Keys über alle Instanzen hinweg sind unabdingbar, um den bevorstehenden gesetzlichen Rahmen einzuhalten – und gleichzeitig ein Höchstmaß an Flexibilität bei der IT-Nutzung zu erreichen. Nur wenn Sicherheit auf diesem Niveau garantiert werden kann, gewinnen Unternehmen zurecht das Vertrauen von Kunden.

James LaPalme

Wie die Sealed Cloud sichere IoT-Angebote ermöglicht

Das Internet of Things ist unaufhaltsam und auch 2018 eines der Top-Themen zur Digitalisierung. Doch neben Chancen lauern auch Gefahren: Mit zunehmender Vernetzung eröffnen sich Hackern und Cyberkriminellen immer mehr Schwachstellen. Kann deutsche Cloud-Technologie helfen, das Internet der Dinge sicherer zu machen?

Das Internet der Dinge (IoT) ist mehr als nur eine Ansammlung vernetzter Kühlschränke: Smart Devices ermöglichen völlig neue Dienstleistungen und bieten Unternehmen Möglichkeiten sich selbst neu zu erfinden. Vor allem die M2M-Kommunikation (Machine-to-Machine) verspricht der Industrie derzeit innovative Geschäftsmodelle. Vernetzte Wertschöpfungsketten im Sinne einer Industrie 4.0,

die ohne menschliches Zutun Daten austauschen und sich selbständig steuern, erlauben es Unternehmen in Zukunft, ihr Service-Portfolio flexibler zu gestalten und Produktionsabläufe mit Losgröße ‚Eins' zu fahren.

IoT: Risiken und Nebenwirkungen?

Doch neben Chancen birgt das Internet of Things natürlich auch Risiken – denn jedes vernetzte Gerät bietet Hackern und Cyberkriminellen eine neue Angriffsfläche. So waren beispielsweise im Juli 2017 Millionen von Überwachungskameras von einer schweren Sicherheitslücke betroffen, die es Angreifern erlaubte, den Videofeed einzusehen oder sogar zu unterbrechen.[1]

Datensicherheit und technischer Datenschutz sind also erfolgskritische Faktoren für praxisorientierte und umfassende IoT-Lösungen: Wesentliche Aufgabe bestehen darin, wertvolles Know-How und Betriebsgeheimnisse zu schützen, bei personenbezogenen Daten, wie sie z.B. durch „wearables" entstehen, den Datenschutz entsprechend dem Stand der Technik zu gewährleisten sowie wettbewerbs- und kartellrechtliche Vorschriften einzuhalten, sowie last , but not least, dafür zu sorgen, dass Angriffe die Produktions- und IT-Infrastruktur nicht beeinflussen oder schädigen können. Die Angriffe durch WannaCry und NotPetya letztes Jahr sind nur 2 Beispiele hierfür.

Dr. Hubert Jäger, CTO, Uniscon GmbH

Dirk Schlesinger, Chief Digital Officer, TÜV SÜD

„Digitalisierung und Vernetzung sind machtvolle Werkzeuge, um Prozesse zu optimieren und neue Geschäftsmodelle zu entwickeln, die Kunden noch mehr Nutzen bringen. Das gelingt aber nur, wenn das Vertrauen im Umgang mit Daten bestehen bleibt. Dann treiben Unternehmen, ihre Arbeitnehmer und Kunden die digitale Transformation selbst mit voran", sagt Dr. Dirk Schlesinger, Chief Digital Officer der TÜV SÜD AG.

Eine Cloud-Technologie für Unternehmen

Mit der vom Bundesministerium für Wirtschaft und Energie (BMWi) geförderten und international patentierten Sealed-Cloud-Technologie des Münchner TÜV SÜD-Partners Uniscon GmbH existiert eine Cloud-Infrastruktur, die Unternehmen einen wichtigen Baustein für die nötige Datensicherheit liefert: „Die Sealed-Cloud Technologie lässt sich einfach in bestehende Systeme integrieren und bildet die Basis für virtuelle Datenräume, über die IoT-Anwendungen, Big-Data-Analysen und M2M-Kommunikation einfach umgesetzt werden können", erklärt Uniscon-CTO Dr. Hubert Jäger.

„Die Anwendungen sind vielfältig", ergänzt Schlesinger. „Von der datenschutzkonformen Auswertung von Videodaten im öffentlichen Raum, der sicheren Verarbeitung von persönlichen Daten in der Medizin über Anwendungen in der Versicherungswirtschaft bis hin zur Verarbeitung von Fahr- und Fahrzeugdaten bei autonomen Automobilen ist alles möglich – und natürlich hochsicher."

Als Beispiel einer möglichen IoT-Anwendung nennen Jäger und Schlesinger das Forschungsprojekt CAR-BITS.de, das die Uniscon GmbH gemeinsam mit der Continental Automotive GmbH, dem Fraunhofer Institut AISEC und der Hochschule Bonn-Rhein-Sieg vorantreibt. Das Projekt soll es ermöglichen, Sensordaten, die über das Auto ermittelt werden, datenschutzgerecht auszuwerten und verschiedenen Anwendungsbereichen anonym zur Verfügung zu stellen – beispielsweise zur Ermittlung des Straßenzustandes oder von stehenden Hindernissen. „Es muss hier unter anderem sichergestellt werden, dass die fahrzeug- und straßenbezogenen Daten zuverlässig von den dazu installierten Sensoren stammen, nicht von Dritten manipuliert und vor allem keine Profile von Personen erstellt werden können", sagt Jäger.

Technischer Datenschutz, der überzeugt

Hier kommt Uniscons Sealed-Cloud-Technologie ins Spiel: Sie sorgt mit rein technischen Maßnahmen dafür, dass die Übertragung und Speicherung von Verkehrsdaten verschlüsselt erfolgt und dass sowohl Daten als auch Verbindungsinformationen während der Verarbeitung geschützt sind. „Andere Cloud-Lösungen kombinieren organisatorische und technische Schutzmaßnahmen. Wir ersetzen die organisatorischen durch technische Maßnahmen. Betreiber und Administratoren werden technisch ausgeschlossen und haben auch bei der Verarbeitung keinen Datenzugriff. Die Verschlüsselung sowie die logische und physische Kapselung der Server stellen sicher, dass niemand unberechtigt zugreifen kann", so Jäger.

Mit diesem Konzept haben die Münchner Cloud-Experten auch die Deutsche Telekom überzeugt: Europas größtes Telekommunikationsunternehmen hat seine Managed Security Services bereits im März 2017 um das Angebot der „Versiegelten Cloud" erweitert, die auf Uniscons einzigartiger Datacenter-Technologie basiert. „Mit Angeboten wie der Versiegelten Cloud stärken wir unsere Position", sagt Dirk Backofen, Leiter Telekom Security. Sein Ziel sei es, Kunden Lösungen vorzuschlagen, die höchste IT- und Datensicherheit gewährleisten. Der Dienst kann selbst für Träger von Berufsgeheimnissen nach §203, wie etwa Ärzten, Anwälten und Behörden verwendet werden.

Dr. Hubert Jäger, Dirk Schlesinger

Referenzen: **[1]** http://blog.senr.io/blog/devils-ivy-flaw-in-widely-used-third-party-code-impacts-millions

IT-Integration – Erfolgsfaktor der Digitalisierung

Die Verlagerung der Legacy-IT in die Cloud nimmt Fahrt auf. Bei Multi-Cloud-Lösungen mit SaaS, IaaS und PaaS bleibt aber die Integration aller Systeme oft auf der Strecke. Dabei ist sie der Schlüssel für nahtlos-digitale Prozesse.

Die Technikgeschichte ist voll von Innovationen, denen erst durch ihre Integration der Durchbruch gelang. Ottomotor, Telefon, Fernseher, Walkman, Faxgerät sowie MP3-Player wurden erst zum ökonomischen Erfolg, als Unternehmer sie mit weiteren Anwendungstechnologien verbanden. Heute sind es digitale Innovationen, die erst durch ihre Integration ihre vollen Potentiale entfalten. Durch Social, Mobile, Analytics sowie Cloud und das Internet der Dinge haben Unternehmen zahllose Potentiale, ihre Geschäftsmodelle anzupassen oder zu erneuern. Aber echte Wettbewerbsvorteile erzielen sie erst mit der Integration aller Teilsysteme – etwa in sogenannten SMACIT-(Social, Mobile, Analytics, Cloud, Internet of Things)-Systemen: Diese integrieren alle Einzeltechnologien unter einem Dach. Erst in der Verbindung verbessern SMACIT die Kundenbindung und ermöglichen die Vernetzung verteilter Daten und Prozesse mit denen von Partnern und Anwendern.

Integration der IT verbessert Produktivität und Workflows

In einer Studie von Ende 2017 wollten Dell Boomi und Vanson Bourne wissen, was die 900 befragten IT-Entscheider zum Thema Vernetzung denken und wie sie bei der Integration ihrer IT-Systeme aufgestellt sind. Als Vorteile nennen 73 Prozent der Befragten steigende Produktivität, 68 Prozent votieren für verbesserte Datenverfügbarkeit, effizientere Arbeitsabläufe geben 57 Prozent an. Zudem hoffen 54 Prozent auf höhere Rentabilität sowie 48 Prozent auf schnellere und genauere Entscheidungen. 88 Prozent wollen durch Integration in den nächsten zwölf Monaten ihren Umsatz steigern. Das Mittel der Wahl ist dabei Integration Platform as a Service(IPaaS). Schon heute haben 43 Prozent der befragten Unternehmen eine solche Plattform im Einsatz. Genau der gleiche Anteil führt IPaaS im Unternehmen ein; weitere acht Prozent der Teilnehmer planen das für das laufende Jahr. Unter den Nutzern von IPaaS geben 74 Prozent an, dass es ihre Unternehmen intelligenter gemacht hat; 72 Prozent meinen schneller und 62 Prozent besser geworden sein.

Customer Engagement und Digitized Solutions nur mit IPaaS realisierbar

Zwei der spannendsten Strategien der Marktgestaltung und Kundenentwicklung sind auch nur durch und mit der Integration in SMACIT-Systemen umsetzbar. Customer Engagement und Digitized Solutions basieren auf der nahtlosen Vernetzung zwischen Kunden und Herstellern und steuern eine personalisierte Interaktion. Customer Engagement bedeutet, dem Kunden über alle Kanäle hinweg ein nahtloses Marken- oder Produkterlebnis zu bieten und dabei eine nachhaltige Bindung an das Unternehmen zu erzeugen. So nutzt beispielsweise Adidas eine App und Cloud-Technologien für ein personalisiertes digitales Engagement mit Verbrauchern. Die App ist vernetzt mit der Adidas Marketing Cloud, Commerce Cloud und Service Cloud. Zu den Features gehören maßgeschneiderte Produktempfehlungen, die Farbvorlieben berücksichtig und die Personalisierung von Produkten. Blogeinträge, Videos und Echtzeit-Updates erhält jeder Nutzer angepasst an seine sportlichen Interessen. Durch Daten und die Fähigkeit, auf die Präferenzen und das Verhalten eines Kunden einzugehen, möchte Adidas zum weltweit führenden Sportproduzent avancieren.

Auch Digitized Solutions basiert auf vernetzten Systemen, bei denen das eigentliche Produkt nur noch Mittel zum Zweck wird. So verkauft ein Autohersteller künftig nicht mehr ein Auto, sondern gewährleistet seinen Kunden eine durchgängige und intermodale Mobilität. Dies funktioniert neben dem Consumer-Markt auch im B2B, wie das Beispiel General Electric (GE) zeigt. Schon seit einiger Zeit verkauft das Unternehmen nicht einfach nur Anlagen wie Turbinen oder Triebwerke. Stattdessen bietet GE heute komplettes Anlagenmanagement an sowie Analyseservices für seine Produkte. Der Nutzwert für die Betreiber steigt beispielsweise durch Predictive Analytics, was ungeplante Produktionsstillstände vermeidet. GE analysiert dafür IoT-Daten, um seinen Kunden bei der Effizienzsteigerung zu helfen, in dem es anstehende Wartungen frühzeitig anzeigt und einleitet. Der Konzern baut außerdem ein Netzwerk von Partnern auf, die ebenfalls Asset-Management und Analyseangebote für Endkunden anbieten.

Silodenken muss endgültig vorbei sein

Customer Engagement wie auch Digitized Solutions benötigen ein belastbares technologisches Rückgrat mit performanten Kapazitäten für die Integration durch SMACIT-Systeme. Diese Infrastrukturen bilden in Zukunft die Voraussetzungen dafür, dass Unternehmen sich im digitalen Zeitalter differenzieren können. Obwohl die Zeichen der Zeit eindeutig sind, haben viele Unternehmen noch nicht erkannt, dass das Silodenken endgültig vorbei sein muss. Wirtschaftlicher Erfolg wird in der Zukunft von der Vernetzung abhängen und in deren Zentrum steht die Integration durch SMACIT-Systeme.

Michael Morton

Michael Morton, Chief Technology Officer Produktentwicklung und Innovation, Dell Boomi

Viele Clouds für viele Aufgaben: Wie der Mittelstand die richtigen auswählt

Verschiedene Clouds zu nutzen, lohnt sich nicht nur für Großunternehmen. Auch der Mittelstand zieht Mehrwert aus dem Einsatz von Multi-Cloud, wenn er es richtig angeht.

In den meisten Unternehmen wächst die IT, denn Mitarbeiter brauchen für ihren Arbeitsalltag eine Vielzahl an Tools und die geeignete Infrastruktur dafür. Da mehr Workloads, Apps und Dienste auch mehr und skalierbare Ressourcen brauchen, setzen Firmen auf die Cloud. Sich auf einen einzigen Cloud Provider festzulegen, fällt schwer – selbst wenn es nur um Infrastructure as a Service (IaaS) geht. Unternehmen, die zusätzlich Platform und Software as a Service (PaaS und SaaS) einbeziehen wollen, kommen meist gar nicht darum herum, mehrere Anbieter zu nutzen.

Der gleichzeitige Einsatz mehrerer Clouds ist nicht nur für Großunternehmen, sondern auch für den Mittelstand sinnvoll. Da in den IT-Abteilungen kleinerer und mittlerer Unternehmen (KMU) aber häufig einzelne Personen mit unterschiedlichen Themen betraut sind, kann sich dort niemand alleine auf den Cloud-Einsatz spezialisieren und fokussieren. Die Digitalisierung muss oft hintanstehen, wenn die Verantwortlichen sich dafür nicht externe IT-Unterstützung holen. Bei Cloud-Services setzen Mittelständler daher auch lieber auf nur eine Lösung, die eine große Themenbreite abdeckt, anstatt mehrerer verschiedener Lösungen, für die jeweils Experten nötig sind.

Peter Fischer, Teamleiter Server & Cloud Infrastructure, Axians IT Solutions

Das ist zu kurz gedacht: Ein einziger Anbieter verfügt nicht für jeden Anwendungsfall über die beste Lösung. Besonders wenn es sich um PaaS und SaaS handelt, fahren Anwender mit verschiedenen, spezialisierten Lösungen besser. Sie erhalten so schneller die gewünschten Ergebnisse und werden dank Muti-Cloud flexibler, denn sie können die jeweils passendsten Cloud-Services bei Bedarf buchen, skalieren und wieder abbestellen. Fehlt dagegen ein solches Angebot, geben Fachbereiche leicht der Verlockung nach, Schatten-IT einzusetzen. Sie buchen dann Cloud-Dienste an der IT-Abteilung vorbei.

Mit den richtigen Services Schatten-IT verhindern

Multi-Cloud, die auf die Wünsche und Bedürfnisse der Anwender eingeht, und strategisch eingesetzt wird, kann Schatten-IT eindämmen. Denn wenn Fachbereiche mit dem offiziellen Angebot der IT-Abteilung zufrieden sind, haben sie keinen Anreiz andere Cloud-Services zu nutzen. Bietet die IT-Abteilung also selbst verschiedene Tools an und reagiert kurzfristig auf Anforderungen der Fachbereiche, fällt die Motivation weg, auf Schatten-IT zurückzugreifen. Da in KMU Multi-Cloud-Fachwissen häufig nicht ausreichend spezialisiert vorliegt und auch die Ressourcen begrenzt sind, setzen sie hier oft auf externe Spezialisten.

Multi-Cloud strategisch angehen

Entscheiden sich KMU, mehr als einen Cloud-Anbieter zu nutzen, lohnt es sich, von Anfang an – schon bei der Entwicklung der Cloud-Strategie – mit einem Cloud-Integrator zusammenzuarbeiten. Er bringt Fachwissen im Cloud-Umfeld mit und hat Erfahrung mit Multi-Cloud-Projekten im Mittelstand. Im ersten Schritt analysiert er den konkreten Bedarf des Unternehmens, beschreibt die Anforderungen und Use Cases. Zudem erhebt der Cloud-Integrator Daten zu bereits genutzten Diensten sowie der vorhandenen Infrastruktur und setzt sich intensiv mit der Motivation des Kunden, Multi-Cloud einzusetzen, auseinander: Wo bestehen Lücken? Was wünschen sich die Mitarbeiter? Hier ist es wichtig, den Bedarf sowohl der IT-Verantwortlichen als auch der Fachabteilungen zu erfragen.

Die Ergebnisse nutzt der IT-Integrator, um Themen und Dienste zu priorisieren und passende Cloud-Anbieter zu ermitteln. Er legt die Vor- und Nachteile unterschiedlicher Angebote etwa für Identity Management, Multifaktor-Authentifizierung oder Backup und Disaster Recovery dar. Auch für Entwicklungsumgebungen, für Tools bei Kommunikation und Collaboration, wie Office365, und Datenbank-Services, kennt der Cloud-Integrator die passenden Anbieter. So müssen KMU die größte Hürde bei Multi-Cloud – die richtigen Angebote zu finden und daraus auszuwählen – nicht alleine nehmen.

Erst auf Basis all dieser Daten entwickelt der Dienstleister gemeinsam mit dem Unternehmen eine geeignete Strategie. Durch dieses Vorgehen vermeiden KMU unnötigen Aufwand, wie er durch den unkoordinierten Einsatz von Cloud-Diensten und damit verbundene Fehler entsteht.

Details zählen

Stehen Anforderungen und Strategie fest, geht es an die Feinauswahl. Cloud-Angebote müssen in die vorhandene Infrastruktur integrierbar sein und mindestens die Sicherheits- und Datenschutzrichtlinien des Unternehmens erfüllen. Es empfiehlt sich, nur zertifizierte Cloud-Anbieter in die engere Auswahl zu nehmen. Dabei ist einzuplanen, dass Sicherheit und Datenschutz auch bei Public-Cloud-Angeboten im Verantwortungsbereich des Anwenders liegen.

Sind geeignete Clouds für die Multi-Cloud ausgewählt und ist für ihre Sicherheit gesorgt, wartet bereits die nächste Hürde: das richtige Bezugsmodell. Schon bei der Auswahl eines passen-

den Modells wird es schwierig. Dabei existieren Bezugsmodelle, die auf den Bedarf im Mittelstand zugeschnitten sind.

Je mehr Clouds der Anwender nutzt, desto aufwendiger werden neben dem Bezugsmodell auch die Verwaltung der Dienste und die Planung der Kosten. Zudem müssen IT-Verantwortliche Rechte vergeben und die Dienste an den jeweils aktuellen Bedarf anpassen. Auch hier lohnt es sich, auf herstellerunabhängige Dienstleister zurückzugreifen. Sie kennen die besten Modelle und beraten fachkundig. Auch auf die durch Multi-Cloud veränderte Aufteilung der Kosten bereiten sie die Anwender vor und bieten eine Übersicht.

Von der Theorie zur Praxis

Stehen Strategie, Sicherheit und Bezugsmodelle für die Multi-Cloud, geht es an die Implementierung. Der Cloud-Integrator unterstützt bei der Migration: Er kennt die Auswirkungen auf die bestehende Infrastruktur, kann nötige Down-Time richtig planen und schafft so die Voraussetzungen für die Migration. Er weiß, wie sich Abhängigkeiten verändern – beispielsweise ist eine stabile, schnelle Internetanbindung essenziell – und welche Prozesse an die Multi-Cloud angepasst werden müssen. Der IT-Dienstleister integriert die Multi-Cloud und hilft im operativen Betrieb. Bei allen Schritten bindet er immer die IT-Mitarbeiter ein, so dass sie die Cloud-Dienste anschließend selbst betreiben können. Darüber hinaus kann er Migration, Integration sowie den operativen Betrieb der Clouds komplett übernehmen. Dann optimiert er zudem kontinuierlich die Infrastruktur.

Multi-Cloud-Umgebungen sind für mittelständische Unternehmen eine nützliche Lösung. Holen sie sich bei der Planung und Einführung externe Unterstützung, finden sie leicht die richtigen Angebote für IaaS, PaaS und SaaS. Ohne selbst umfangreiches Fachwissen aufbauen zu müssen, setzen sie auf ihren Bedarf abgestimmte Cloud-Services flexibel ein. Bei Bedarf können sie auch den Betrieb der unterschiedlichen Clouds auslagern. Peter Fischer