

iX *extra* November 2020 **Hosting**

Eine Sonderveröffentlichung der Heise Medien GmbH & Co. KG

Hosted Managed Services im Unternehmenseinsatz

IT-Infrastruktur nach eigenen Vorgaben
extern betreiben lassen

Ideal kombiniert

Seite 110

Servermanagement mit Redfish

Seite 114

Managed Cloud zu Hause:
AWS, Azure Stack und Anthos

Seite 116

Service-Management nach ITIL

Seite 118

Deutsche Hosting-Provider
mit Managed Services

Seite 120



iX extra zum Nachschlagen:
www.ix.de/extra

Ideal kombiniert

Hosted Managed Services im Unternehmenseinsatz

Der Weg in die Cloud ist zwar kurz und bequem, aber die Anwender geben damit auch die Kontrolle darüber ab, was mit ihren Daten passiert.

Das passt nicht immer zu den rechtlichen oder organisatorischen Vorgaben von Unternehmen. Das Betreiben einer kompletten Infrastruktur in einem eigenen Rechenzentrum (on Premises) bedeutet jedoch einen hohen Aufwand. Managed Services von einem Hoster sollen das Beste beider Seiten miteinander verknüpfen.

Die Cloud nagt am klassischen Hosting-Geschäft. Dass sich die Kunden immer weniger mit den Details der Infrastruktur befassen wollen, birgt aber auch Chancen: Die Provider können ihre Wertschöpfung durch zusätzliche Dienstleistungen erweitern. Hierfür sind Managed Services das zentrale Produkt. Die Kunden bestimmen die Infrastruktur und kontrollieren ihre Daten. Für Monitoring, Updates, Verfügbarkeit, Backups und nicht zuletzt die IT-Sicherheit ist hingegen der Hoster zuständig.

Fast so alt wie das Internet ist der Begriff des Managed-Service-Providers (MSP). Heute ist er aus der Mode gekommen, weil praktisch alles „Managed“ ist und jeder Hoster auch diese Variante im Portfolio hat.

Managed Services erlauben eine abgestufte Aufteilung der Betriebsaufgaben zwischen Provider und Kunden. PlusServer zum Beispiel definiert hierfür drei Management-Levels. Beim Infrastructure Management behält der Kunde die vollen Administrationsrechte. Der Hoster kümmert sich um einen zuverlässigen Betrieb der Hardware und behebt Störungen an

der Netzinfrastruktur. Das ist ideal für alle, die selten Unterstützung benötigen und ihre IT zwar extern, aber dennoch in Eigenregie betreiben. Zusätzliche Leistungen können bei Bedarf hinzugebucht werden.

Die mittlere Stufe – Operations Management Level – sieht

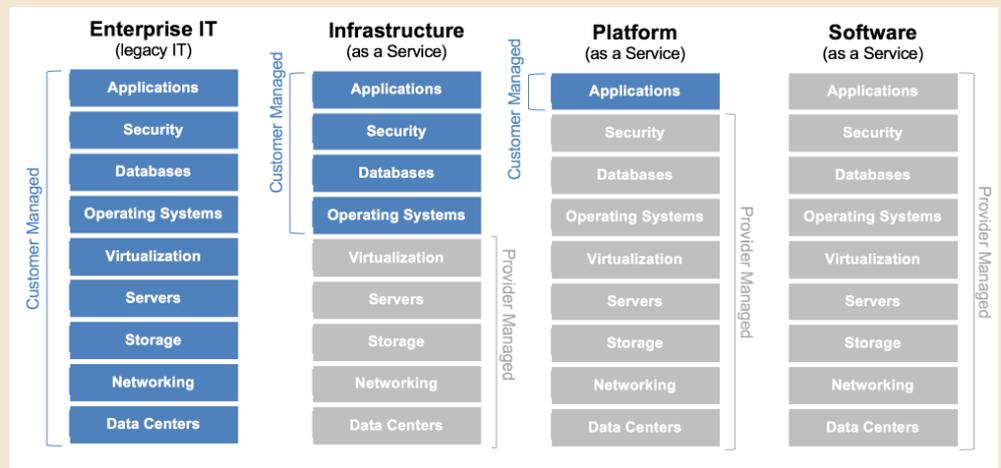
eine Teilung der Administrationsrechte vor: Der Provider entstört das System und die Serverdienste; über Sicherheitsupdates wird der Kunde informiert und kann entscheiden, ob und wann er diese einspielen will.

Beim Service Management Level schließlich ist der Hoster

für den jeweiligen Dienst komplett verantwortlich und kümmert sich um alle untergeordneten Ebenen (siehe Abbildung 1).

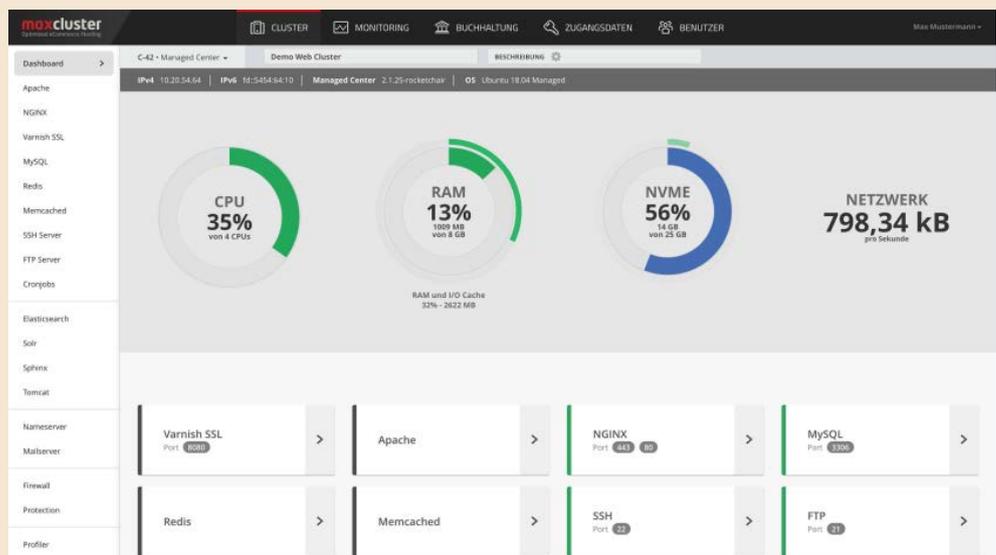
Monitoring und Troubleshooting

Die Aufgaben eines Managed-Service-Providers lassen sich grob in drei Bereiche unterteilen: vorbeugende Maßnahmen, Monitoring und Troubleshooting mitsamt schneller Wiederherstellung von Diensten. Zu ersteren gehören automatisierte Backups, die Aktualisierung von Software durch Bugfixes, Sicherheitsupdates und gegebenenfalls auch Upgrades auf neue Versionen. Ob dies in Absprache mit den Kunden stattfindet, hängt vom vereinbarten Service Level ab. Insbesondere bei größeren Softwarepaketen ist eine detailliertere Vereinbarung darüber nötig, für



Verantwortlichkeiten lassen sich auf unterschiedliche Weise zwischen Provider und Kunden aufteilen (Abb. 1).

Managed Center zeigt alle Informationen zu einem Managed Service auf einen Blick (Abb. 2).



welche Komponenten welche Updateregeln gelten. So unterscheidet der WordPress-Spezialist HostPress zwischen automatischen Security-Patches ohne Versionsupdates und einem speziellen SecurePlan-Service, der nicht nur die Kernsoftware aktualisiert, sondern auch Vorlagen (Themes) und Plug-ins. Hierfür ist ebenso manuelle Arbeit notwendig wie für die abschließenden Funktionstests.

Die größten Unterschiede zwischen den Providern gibt es beim Monitoring, vor allem hinsichtlich der Software. Hier geht es nicht nur darum, welche Anwendungen überwacht werden, sondern auch, in welchen Intervallen, auf welcher Ebene und mit welchen Maßnahmen. Ein erfolgreicher Ping auf einen Port garantiert noch keine fehlerfreie und performante Applikation. Je ähnlicher der Test einer echten Kunden-Transaktion ist, desto besser (siehe Abbildung 2).

Zum Überwachen der zahlreichen Parameter setzen Hoster oft auf mehrere Tools und selbst geschriebene Skripte. Netways und Thomas-Krenn nutzen die deutsche Monitoringsoftware Icinga mit einem selbst entwickelten Open-Source-Webinterface (siehe Abbildung 3).

Monitoringmaßnahmen am Beispiel maxcluster

Kategorie	Umsetzung
Ressourcenmonitoring	minütliche Überwachung von CPU, RAM und SSD
Websiteperformance	externes Monitoring mit Ping und HTTP
Application-Monitoring	Überwachung wichtiger Parameter der Dienste Varnish, Apache, MySQL und Redis
VPN-Monitoring	IPsec-Wartung und Überwachung der Verbindung

Neben der eigentlichen Anwendung gilt es manchmal auch, Hardware- oder Umgebungsparameter im Blick zu behalten. Thomas-Krenn bietet hierfür spezielle Monitoringhardware an. Hierzu gehören SNMP-fähige Sensoren, SMS-Gateways und Umsetzer beliebiger Digitaleingänge auf Ethernet.

Bestand die Fehlerbehebung beim Provider in der Vergangenheit vor allem im schnellen Austausch von Servern, Festplatten oder anderen Komponenten, so rückt dies in Zeiten der Virtualisierung auf der Prioritätenliste weiter nach hinten. Sofern die Dienste durch Cluster- und Redundanzkonzepte nicht unbeeindruckt weiterarbeiten, lassen sie sich in vielen Fällen schnell auf einen anderen Server verschieben oder als neue Instanz starten.

Diese Vorgänge laufen meist automatisiert und es kommen zunehmend Orchestrierungswerkzeuge zum Einsatz. So erlaubt der Containermanager

Kubernetes Festlegungen darüber, wie viele Instanzen eines Dienstes jeweils aktiv sein sollen, und der integrierte Replication Controller startet sie im Fehlerfall neu.

Auch beim Ausfall eines dedizierten Servers tauschen Hoster kaum noch sofort, sondern schalten einfach ein anderes Gerät aus der Reserve frei. Es entlastet nicht nur das Personal, sondern senkt auch das Fehlerisiko, wenn der Austausch nicht spontan um drei Uhr nachts, sondern geplant am nächsten Werktag stattfindet.

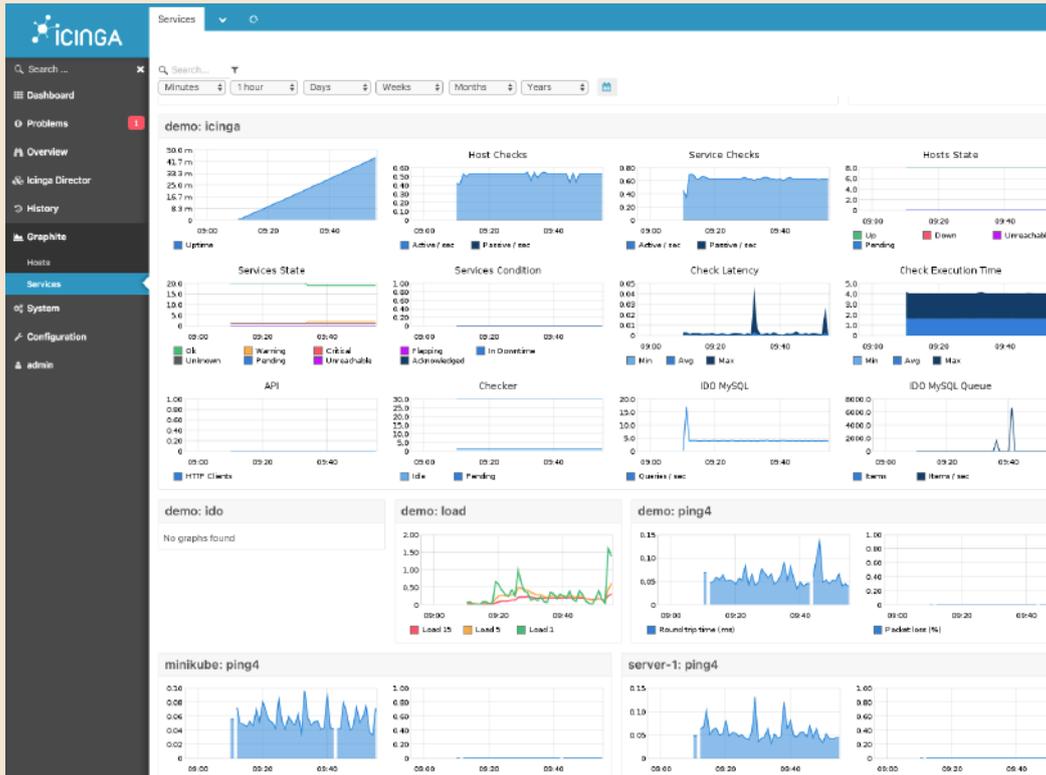
Je nach konkretem Anwendungsfall können Managed Services eine Reihe weiterer Leistungen umfassen, etwa Softwareoptimierungen (Cyberwebhosting) oder Performancetests (DM Solutions). Die Provider versuchen, möglichst viele Aufgaben zu automatisieren, stoßen aber auch an Grenzen, etwa beim Entwickeln von Skripten oder beim Auswerten von Logfiles. Wo manuelle Aufgaben nicht pau-

schalisiert in einem Managed Service enthalten sind, werden Techniker oder Entwickler oft auf Stundenbasis angeboten.

Managed Infrastructure

Zu den ältesten und am weitesten verbreiteten Managed-Hosting-Produkten gehören Managed Server, wahlweise als dedizierte oder virtuelle Variante. Häufig ist das Management inzwischen Standard oder man kann es zu den einzelnen Paketen hinzubuchen – teilweise auch im Nachhinein (DM Solutions). Darüber hinaus lassen sich nahezu alle anderen Geräte vom Hoster managen: von Storage und Load Balancern über Firewalls und Switches bis zu Managed Colocation.

In aller Regel handelt es sich nicht um einzelne Geräte, sondern um eine komplette Infrastruktur. Weit verbreitet sind Managed Cluster, die aus mehreren Servern im Verbund mit Load Balancern bestehen. Ist eine Lastverteilung nicht nötig, können Hochverfügbarkeitscluster auch ohne Load Balancer realisiert werden. Host Europe und Strato bieten hierfür die Funktion Cluster IP an, mit deren Hilfe eine feste IP-Adresse durch Umschalten



Quelle: Netways

Die deutsche Monitoringsoftware Icinga kommt bei diversen Hostern zum Einsatz (Abb. 3).

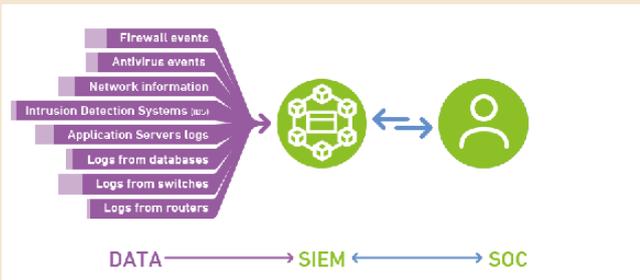
zunehmend der Tatsache Rechnung, dass Unternehmen kaum alle Anwendungen an einem Standort und bei einem Dienstleister betreiben. Fritz Managed IT etwa bezieht in seine Managed Server auch Geräte und vServer ein, die bei einem anderen Hostler stehen. Gründe für ein solches Szenario können gewachsene Strukturen, regionale Aspekte oder Sicherheitsanforderungen sein.

Aber auch außerhalb des Rechenzentrums können Provider Kundeninfrastrukturen betreiben – Managed WLANs zum Beispiel. Sie sind vor allem als Gastzugänge in Geschäften, Restaurants und öffentlichen Gebäuden beliebt. Die doppelte Infrastruktur parallel zum meist bereits vorhandenen internen Netz erhöht nicht nur Sicherheit und Durchsatz. Der Provider übernimmt auch weitere Aufgaben wie den Betrieb des Gästeportals, Werbeeinblendungen und gegebenenfalls die Rechnungsstellung.

Managed Cloud

Während viele Hostler Cloud-Services anfangs als Bedrohung angesehen haben, etablieren sie mittlerweile immer mehr komplementäre Geschäftsmodelle. Einige Managed Services lassen sich ohnehin nicht durch Cloud-Dienste ersetzen: Viele Unternehmensanwendungen sind gar nicht Cloud-fähig, müssen aber noch jahrelang weiterlaufen.

IT-Security muss auf allen Ebenen sichergestellt werden (Abb. 5).



Quelle: Leaseweb

Ein Managed Security Operations Center (SOC) aggregiert Informationen aus allen möglichen Quellen (Abb. 4).

verschiedenen Servern zugeordnet werden kann. Damit lassen sich einfache Failover-Konfigurationen realisieren, Upgrades unterbrechungsfrei

einspielen oder Wechsel zwischen Live- und Entwicklungssystem bewerkstelligen. Kunden können die Konfiguration mithilfe eines Verwaltungstools

(meist Plesk) selbst vornehmen. Dabei müssen die Server nicht derselben Produktkategorie angehören, es ist auch ein Cluster mit dedizierten und virtuellen Servern möglich.

Managedhosting.de bietet Disaster Recovery as a Service an, basierend auf Backup- und Recovery-Produkten von Veeam und VMware. Damit lässt sich sowohl eine regelmäßige Auslagerung von Datensicherungen realisieren als auch eine vollständige Replikation kritischer Anwendungen als Notfallvorsorge.

Serviceprovider tragen mit ihren Managed Services

Quelle: Adacor

Organisation	VDA ISA Stufe 3	ISMS	Datenschutz-Management	Jährliche Verpflichtungen	Jährliche Schulungen	Interne Revision	Compliance Management
Betrieb	IDW PS 951 Typ 2	Security Team	Patch Management	Incident Response	24/7 Bereitschaft	Fachpersonal	Persönlicher Project Lead
Plattform	ISAE 3402 Type 2	Systemhärtung	Monitoring	Vulnerability Scanning	Web Application Firewall		
Hardware	ISO 27001 Audit in 2018	24h Hardware Tests	Individuelle Server	Sichere Entsorgung			
Netzwerk		VPN	Netz-Segmentierung	DDOS Protection	Firewalls	Intrusion Detection	2 Faktor Auth.
Rechenzentrum	ISO 27001	Zutrittskontrollen	Brandschutz	Tier 3/4 USV	Notstrom	Standort Frankfurt	24/7 Leitstelle

Managed Services

Die meisten Managed-Cloud-Angebote gibt es für AWS. Nicht immer erschließt sich aus den Produktnamen, was sich dahinter verbirgt. Managed AWS umfasst generell die Einrichtung und den Betrieb einer AWS-Umgebung. Claranet zum Beispiel fasst seine Managed Services für AWS jedoch weiter: Hier gehören Planungsaufgaben wie Cloud Readiness, Compliance und Security Assessments zum Paket.

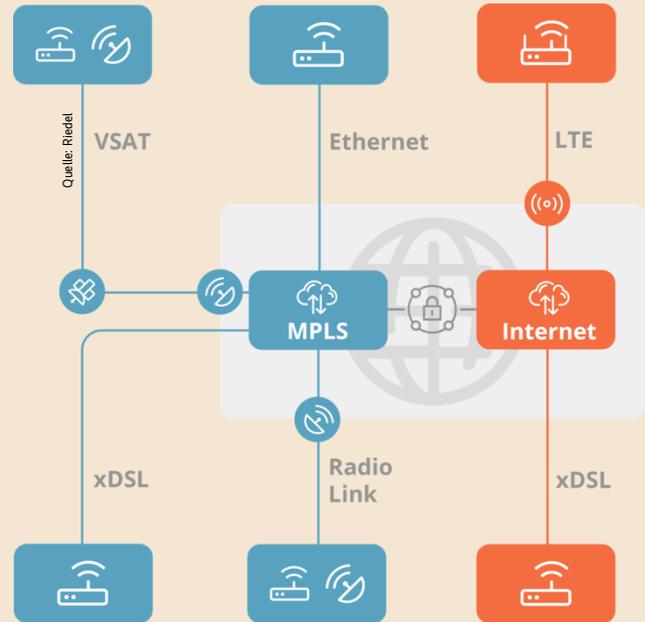
Immer häufiger kommen statt virtueller Maschinen Container zum Einsatz. Es liegt in der Natur dieser Technik, dass ein klassisches Management von Betriebssystem und Softwarestack nicht nötig ist. Statt Updates und Patch-Management werden einzelne Container komplett ausgetauscht. Genau das macht die Technik so attraktiv für neue Anwendungen. Einzelne Container können aber nur überschaubare Aufgaben übernehmen, sodass eine große Anzahl von Instanzen nötig ist. Diese lassen sich nur mit Orchestrierungswerkzeugen betreiben. Seit Docker Swarm nicht mehr weiterentwickelt wird, dominiert hier Kubernetes. Da sich Container damit einfach über unterschiedliche Lokationen verteilen lassen, bietet sich Managed Kubernetes an, wie

Managed SD-WANs nutzen beliebige Zugangstechnologien (Abb. 6).

es IONOS oder ScaleUp im Portfolio haben. Managed Server mit vorinstallierter Docker-Plattform gibt es bei WebhostOne.

Managed Security

Ein recht neues Betätigungsfeld für Provider sind Managed Security Services. War es in der Vergangenheit weitgehend Konsens, dass ein Unternehmen Sicherheitsaspekte nur intern



Systemhäuser und Systemintegratoren mit Managed Services

Systemhaus	Webseite	Produkte
Arvato	www.arvato-systems.de	Managed Services, Application Management
Axians	www.axians.de	Software Asset Management, Managed Data Center, Managed Software, Managed Security, Managed Cloud, SAP Ad hoc Managed Services, Managed WLAN
Bechtle	www.bechtle.com	IT Managed Services, Business Applications, Cloud Services
Cancom	www.cancom-pironet.de	Managed Applications (SAP, MS Dynamics, Desktop as a Service)
Computacenter	www.computacenter.com	Managed Security Services, Virtual Desktop, Service Desk, diverse Managed Services
Logicalis	www.de.logicalis.com	Managed WAN, Managed WLAN, Application Performance Management
Materna	www.materna.de	Managed Workloads (DevOps, IAM, ITSM), Enterprise Service Management, Customer Journey Management
NTT Communications	www.ntt.com	Operations Management, Managed Security, SD-WAN, Desktop as a Service, Identity and Access Management
PIK AG	pik.de	Managed Videoconferencing und Medientechnik
T-Systems	www.t-systems.com	Managed AWS, Managed Azure, Managed VMware, Managed PaaS und Big Data, Multicloud Management

Servermanagement mit Redfish

Um Server kostengünstig betreiben zu können, ist die Möglichkeit eines Fernzugriffs unabdingbar. Dieser sollte auch dann noch funktionieren, wenn es Probleme mit dem Betriebssystem oder Teilen der Hardware gibt. Gängige Remote-Tools wie SSH oder TeamViewer greifen zu kurz, denn auch ein Hardware-Reset, das Flashen einer neuen Firmware, Änderungen von BIOS-Einstellungen oder die Installation eines neuen Betriebssystems sollen remote möglich sein. Hierfür ist zusätzliche Hardware erforderlich und idealerweise auch ein dedizierter Kommunikationskanal, meist in Gestalt eines weiteren Ethernet-Ports. Die Mitbenutzung der vorhandenen LAN-Ports (Pass Through) setzt ein geeignetes Betriebssystem voraus und schränkt daher den Funktionsumfang ein.

Mehr als zwei Jahrzehnte lang fand das ursprünglich von Intel, Dell und HP entwickelte Intelligent Platform Management Interface (IPMI) für die Serverfernwartung Verwendung. Inzwischen steht es insbesondere wegen seiner erst nachträglich eingeführten Sicherheitsfunktionen in der Kritik, aber auch die Softwarearchitektur ist nicht mehr auf der Höhe der Zeit. Deshalb wird es zunehmend durch den von der Distributed Management Task Force (DMTF) entwickelten Nachfolgestandard Redfish abgelöst, der genau diese Schwachstellen beheben soll.

Auf der Hardwareseite sind nur geringe Änderungen nötig. Wie bisher bildet ein Baseboard Management Controller (BMC) das Herzstück der Lösung. Er ist mit den zentralen Komponenten des Servers sowie mit Sensoren für Temperatur, Spannung und Lüfterumdrehungen über ein Bussystem verbunden. Darüber sammelt er Daten und verteilt in umgekehrter Richtung Steuerungsbefehle wie ein Reboot. Deshalb ist der BMC inzwischen nahezu immer direkt auf dem Mainboard verbaut. Bis auf einen Austausch von Hardware können alle Aktionen remote stattfinden, für die sonst ein Techniker vor Ort nötig wäre. Da jeder Serverhersteller seine eigene BMC-Firmware entwickelt, arbeiten Google, IBM, Intel und Microsoft am Open-Source-Projekt OpenBMC.

Völlig neu definiert Redfish die Datenmodelle und Übertragungsprotokolle. Im Mittelpunkt stehen eine REST-API, das offene und effiziente

JSON-Datenformat sowie das Open Data Protocol (ODATA). Die Sicherheit gewährleisten TLS-Verschlüsselung und abgestufte Zugriffsrechte (siehe Abbildung 7).

Damit eignet sich Redfish für das Management großer Serverfarmen mit Tausenden von Geräten. Neben Überwachung und Troubleshooting rücken Automatisierungsaufgaben immer mehr in den Vordergrund. Hierfür können Skripte genutzt werden und es existieren Schnittstellen zu ähnlichen Managementwerkzeugen für Storage (SNIA Swordfish) und Netzwerk-Switches (IETF YANG).

Die großen Serverhersteller verbauen eigene BMCs und ihre Managementtools gehen über die Redfish-Spezifikation hinaus. Bei HPE heißt das Integrated Lights-Out (iLO) und bei Dell EMC Integrated Dell Remote Access Controller (iDRAC). Einige Hostler stellen sie mit ihren dedizierten Servern zur Verfügung. So ist bei PlusServer bereits eine iLO-Advanced-Lizenz enthalten, bei ScaleUp iDRAC8 Enterprise. Ob die Administratoren des Kunden, des Hosters oder beide Zugriffsrechte erhalten, hängt vom gebuchten Servicepaket ab.

Quelle: Thomas-Kreim

Rechte (Priviledges)	 Rolle "Administrator"	 Rolle "Operator"	 Rolle "ReadOnly"
Login	✓	✓	✓
ConfigureSelf	✓	✓	✓
ConfigureComponents	✓	✓	
ConfigureManager	✓		
ConfigureUsers	✓		

Unterschiedliche Rollen ermöglichen abgestufte Privilegien für Administratoren (Abb. 7).

umsetzen kann, reift doch inzwischen die Erkenntnis, dass spezialisierte Dienstleister dies nicht nur ebenso gut, sondern in bestimmten Aspekten sogar besser beherrschen. Ihre umfangreichen Erfahrungen können in viel größere Datenbasen mit Bedrohungsszenarien einfließen und allen Kunden zugutekommen. Zudem sind Experten rar und teuer und mit spezialisierten Tätigkeiten in kleineren Unternehmen nicht ausgelastet.

Immer mehr Hostler versuchen daher, ihr über viele Jahre gesammeltes Know-how im Bereich Security als Managed Services anzubieten. Ein Beispiel hierfür ist ein Managed Security Operations Center (SOC), wie es sepago und Leaseweb zur Verfügung stel-

len. Hier überwacht ein Team von Spezialisten rund um die Uhr den Sicherheitsstatus, um Schwachstellen, Eindringlinge oder verdächtige Ereignisse zu erkennen. Daraus werden im Fall der Fälle sofort umsetzbare Maßnahmen abgeleitet. Die Grundlage bildet eine Software für das Security Information and Event Management (SIEM), die eine Echtzeitanalyse von Sicherheitswarnungen ermöglicht und mittels einer Korrelations-Engine alle netzwerk-basierten Ereignisdaten und Protokolldateien integriert, um Schwachstellen und Anomalien zu erkennen (siehe Abbildung 4).

Leaseweb und Axians beschäftigen darüber hinaus ein Computer Emergency Re-

sponse Team (CERT), das im Falle eines sicherheitsrelevanten Geschehens das Krisenmanagement übernimmt und forensische Untersuchungen, Reparaturen sowie Gegenmaßnahmen einleitet.

Managed Server sind in der Regel schon in der Basisversion mit einfachen Sicherheitsfunktionen ausgestattet. Bei Hetzner gehören dazu die signaturbasierte Abwehr bekannter Würmer und wörterbuchbasierter Brute-Force-Angriffe. Logfiles werden viertelstündlich ausgewertet und bei Anomalien gehen Reports direkt an Hetzners Service Center.

Darüber hinaus können die Kunden alle Security-Maßnahmen, die in Unternehmen State of the Art sind, auch als Ma-

naged Services beziehen. Hierzu gehören Unified Threat Management (UTM), Intrusion Detection und Prevention (IDS/IPS) oder die Abwehr von DDoS-Angriffen mittels Deep Packet Inspection (siehe Abbildung 5).

Kaum ein Unternehmen besitzt noch Standleitungen oder betreibt ein WAN in Eigenregie. Deshalb sind Managed WANs ein langjährig bewährter Providerservice. Die technische Grundlage bilden in der Regel MPLS-Netze (Multiprotocol Label Switching), die für den Transport geschäftskritischer Daten entwickelt wurden. Im Gegensatz zum Internet, wo IP-Routing dynamisch den Weg bestimmt, gibt MPLS die Pfade vor, sodass eine verbindungsorientierte Übertragung statt-

findet. Damit lassen sich nicht nur Daten unterschiedlicher Kunden durch MPLS-VPNs sicher voneinander trennen, es sind auch echte QoS-Mechanismen (Quality of Service) möglich: Latenz, Laufzeitverhalten und Paketverluste lassen sich genau passend zum Bedarf

steuern. Im Hinblick auf den Trend zu Videokonferenzen und IP-Telefonie ist MPLS also gut gerüstet. Allerdings hat das im Wortsinne auch seinen Preis.

Andererseits ist die Kommunikation mit Messengern und Teams-Räumen wenig

anspruchsvoll und an eine schlechte Videoqualität haben sich die Anwender in Coronazeiten gewöhnt. Aber seit das Homeoffice boomt, benötigen Firmen mehr Flexibilität bei der Anbindung ihrer Mitarbeiter.

Deshalb steigt der Bedarf an WANs, die alle Anschlusstechni-

ken (DSL, Kabel, LTE) gleichermaßen zu einer homogenen Lösung vereinen. Der Katalysator hierfür ist die Entwicklung von Software-defined WANs (SD-WAN), sprich: zentral gesteuerten, virtualisierten Netzwerkfunktionen. Das schafft mehr Flexibilität bei Veränderun-

Managed Cloud zu Hause

Auch die Hyperscaler haben erkannt, dass Unternehmen nicht ihre gesamte IT in die Cloud verlagern werden. Wohl aber wünschen sie sich ein durchgehendes Management, unabhängig davon, wo die Hardware steht. Deshalb öffnen die globalen Cloud-Provider ihre Angebote für Server in den Rechenzentren der Kunden, um so hybride Umgebungen zu schaffen. Dabei gehen sie unterschiedliche Wege.

AWS Outposts

Amazon setzt für AWS traditionell auf nach eigenen Vorgaben gefertigte Whitelabel-Hardware. Davon wird auch nicht abgerückt, wenn die Webservices beim Kunden laufen. Amazon verschickt vorkonfigurierte 42-Zoll-Racks mit Servern, Storage und Switches und erledigt auch die Anschlussarbeiten beim Kunden. Die kleinste Variante passt in ein Vierterack, größere belegen mehrere komplette Racks. Hosters stellen passende Colocation-Räumlichkeiten zur Verfügung.

Je nach individuellen Anforderungen kann sich der Nutzer seine Hardwarekonfiguration an der AWS-Konsole selbst zusammenstellen. Die lokale Outposts-Installation wird dauerhaft per Direct Connect oder VPN mit der nächstgelegenen AWS-Lokation verbunden – in Deutschland sind das Berlin, Düsseldorf, Frankfurt oder München. Hier schließt sich der Kreis zu den von Amazon beworbenen Einsatzszenarien: Anwendungen mit Anforderungen an geringe Latenz.

Darüber hinaus lassen sich so auch Datenschutzvorgaben erfüllen und eigene Last- und Redundanzkonzepte aufbauen. Der Nutzer hat nur Zugriff auf die AWS-Dienste wie EC2 (Compute), EBS (Storage) oder ECS/EKS (Container), nicht aber auf das Betriebssystem oder gar die Hardware. Noch in diesem Jahr soll es auch eine VMware-Variante für Outposts geben. AWS überwacht und verwaltet die Außenstellen so, als befänden sie sich in der AWS-Cloud, und spielt automatisch alle Updates ein. Damit steht Outposts exemplarisch für einen Fully-managed Service on Premises.

Besteht zeitweise keine Verbindung zur AWS-Cloud, so ist nur der Betrieb der Control Plane unterbrochen, während die lokalen Workloads weiterarbeiten. Einige wenige Dienste können auch temporär offline laufen, etwa zur mobilen Datenerfassung und -vorverarbeitung. Hierfür kommt eine spezielle Hardware – Snowball Edge – zum Einsatz.

Microsoft Azure Stack

Einen anderen Weg geht Microsoft, das im Rechenzentrum traditionell mit den großen Hardwareherstellern zusammenarbeitet. Für Microsoft Azure Stack gibt es ein Zertifizierungsprogramm und die Top 5 der Serverlieferanten (Cisco, Dell, Fujitsu, HPE, Lenovo) liefern vorkonfigurierte Systeme. Diese schließen gemeinsame Supportkonzepte ein. Hosting-Provider, die auf Markenhardware setzen, bieten Azure Stack zu-

nehmend auch direkt an (Leaseweb, myLoc, PlusServer). Technisch gesehen ermöglicht es eine ähnliche Hybrid-Cloud wie AWS Outposts. Hierfür werden drei Versionen unterschieden: Neben der klassischen Variante für das Rechenzentrum (Azure Stack Hub) gibt es Azure Stack Edge für IoT- und Edge-Anwendungen. Azure Stack HCI wiederum eignet sich für hyperkonvergente Systeme mit skalierbaren Hochleistungs-Workloads (siehe das Tutorial in iX 9 und 10/2020). Verbindungen zu AWS und Google Cloud werden über einen zusätzlichen Management-Layer (Azure Arc) hergestellt.

Anders als AWS bietet Microsoft einen Disconnected Mode für einen dauerhaften Offlinebetrieb. Damit gehen aber wesentliche Vorteile des Konzeptes wie laufende Updates und ständiges Management verloren.

Google Anthos

Noch flexibler gestaltet Google die Weiterentwicklung seiner Cloud Service Platform (CSP) unter dem neuen Namen Anthos. Sie kann auf beliebiger Hardware im Rechenzentrum installiert werden, arbeitet aber nicht autonom on Premises, sondern nur im Verbund mit der Google Cloud. Einziger gegenwärtig implementierter Hypervisor ist vSphere; mit Cisco besteht eine Kooperation zur Installation auf Hyperflex. Geplant ist die Integration eines eigenen Load Balancers; bisher wird mit externen Geräten gearbeitet.

Google Anthos basiert auf der Google Kubernetes Engine (GKE) und stellt damit Container in den Mittelpunkt der Services. Virtuelle Maschinen können mit Anthos Migrate in Container migriert werden. Weitere Dienste sollen hinzukommen, beispielsweise Istio als Managementplattform für Microservices. Schnittstellen zu AWS und Azure sind bereits integriert, sodass sich Anthos auch als Multicloud-Plattform eignet.

Da alle Lösungen für eine ständige Verbindung mit dem nächstgelegenen Knoten des Hyperscalers konzipiert sind, können sie ihre Vorteile nur ausspielen, wenn sie nicht auf den WAN-Strecken ausgebremst werden. Deshalb entstehen immer mehr direkt geschaltete Leitungen zwischen den Rechenzentren großer Kunden und denen der Cloud-Provider. Bei Amazon heißt dies Direct Connect, bei Microsoft Azure ExpressRoute und bei Google Cloud Interconnect.

Große Colocation-Anbieter wie e-shelster, Interxion und ITENOS verfügen in Deutschland bereits über entsprechende Direktverbindungen. Deshalb spricht vieles dafür, die Cloud-Boliden dort unterzustellen.

Eine Alternative ist ein direkter Port an einem der fünf DE-CIX-Knoten in Deutschland. Ein Service namens DirectCLOUD erlaubt das Aufspannen von VLANs zu verschiedenen Cloud-Providern mit nur einem Vertrag. Einen ähnlichen Service bietet TelemaxX mit Cloud Connect. Über eine Leitung lassen sich unterschiedliche Cloud-Dienste direkt erreichen.

Managed Services

gen und vereinfacht die Systemverwaltung. Als Overlay kann SD-WAN eine Kombination unterschiedlicher Anbindungen nutzen und natürlich auch MPLS einbeziehen (siehe Abbildung 6).

Den Nachteilen bei QoS setzt SD-WAN Application-based Routing (Priorisierung einzelner Anwendungen) und Performance-based Routing (Auswahl der Verbindungen nach Performanceparametern wie Latenz und Jitter) entgegen.

Die Entwicklung von SD-WANs setzt die etablierten MPLS-Netze unter Druck. Beide Verfahren ergänzen einander, aber das Wachstum findet in den SD-WANs statt: Frost & Sullivan zufolge bis 2023 jährlich um fast 50%, während MPLS-Netze stagnieren.

Da beide Weitverkehrsnetze unterschiedliche Anwendungsfälle abdecken, sind für viele

Unternehmen hybride Implementierungen sinnvoll. Der Übergabepunkt der Daten ist derselbe, denn in der Regel gehört der WAN-Router beim Kunden noch dem Provider (Customer Premises Equipment, CPE).

Managed Applications

Synonym verwenden Provider häufig die Begriffe Managed und Hosted Applications. Auch wenn der Nutzer keine oder nur geringe Unterschiede bemerkt, sind doch verschiedene Modelle möglich. Bei einem Managed Service läuft für jeden Mandanten eine separate Softwareinstanz. Die Lizenzen kann entweder der Kunde selbst oder der Hostler beschaffen, ebenso die Update- und Wartungsverträge mit den Softwareherstellern. Tralios

lässt dem Kunden die Wahl zwischen beiden Varianten.

Die Lizenzverwaltung, in vielen Firmen ein leidiges Thema, kann der Dienstleister auch ganz übernehmen. So offeriert Axians einen OneSAM (Software Asset Management) genannten Service, der sich von der einfachen Dokumentation bis zum kompletten Lifecycle-Management abtufen lässt. Software lässt sich individuell managen: Für den einen Kunden bedeutet das, alle Softwareupdates zeitnah einzuspielen, für einen anderen nur Bugfixes und keine Upgrades. Es besteht auch die Möglichkeit, dem Hostler die Entscheidung zu überlassen. Individuelle Service-Level-Vereinbarungen sind für große Installationen die Regel.

Für Hosted Applications hingegen nutzen meist mehrere Kunden eine mandantenfähige

Plattform. Die Managementleistungen sind klar definiert und für alle Mandanten identisch. Ein Beispiel für Software, die Hostler in beiden Varianten anbieten, ist Microsofts Exchange (siehe auch Seite 75).

Eine dritte Möglichkeit realisiert Software as a Service. Hier steht die Software nach einem Pay-per-Use-Modell zur Verfügung und die Managementarbeiten finden im Hintergrund statt.

Je stärker sich ein Anbieter auf eine Applikation fokussiert, desto breiter ist in der Regel sein Dienstleistungsangebot rund um diese Software, unter anderem kundenspezifische Konfiguration (Customizing), Datenverwaltung, Training und Dokumentation. Wer zusätzliche Services rund um die Software nutzen möchte, ist hier am besten aufgehoben. Ein

Service-Management nach ITIL

Während sich Hardware- und Softwareparameter einfach vergleichen lassen, ist es beinahe unmöglich einzuschätzen, wie die internen Prozesse eines Serviceproviders ablaufen. Dabei sind gerade diese ein maßgeblicher Faktor im Fehlerfall, denn Entstör- und Eskalationsprozeduren beweisen ihre Funktionstüchtigkeit eben erst dann. Vor allem die ständigen Änderungen an der IT-Infrastruktur – sei es durch Entstörung, Upgrades oder Erweiterungen – sind potenzielle Fehlerquellen.

Deshalb werben RZ-Betreiber damit, ihre Prozesse an den Vorgaben von ITIL auszurichten. Die IT Infrastructure Library (kurz ITIL) ist ein Framework von Best Practices für den Betrieb technischer Infrastrukturen, das über einen längeren Zeitraum federführend von der später mehrmals umbenannten britischen Regierungsbehörde Central Computing and Telecommunications Agency (CCTA) entwickelt wurde. Inzwischen liegen die Rechte mehrheitlich bei der Firma Axelos, die Schulungen und Zertifizierungen anbietet. Es existieren auch andere IT-Management-Frameworks wie Cobit, FitSM und eTOM, die aber weniger praktische Relevanz erlangt haben.

ITIL beschreibt und strukturiert alle im IT-Management nötigen Prozesse (siehe Abbildung 8). Damit sollen insbesondere die „weichen“ Faktoren (Dokumentation, Qualifizierung, Tools) analysiert und verbessert werden. Denn hohe Verfügbarkeit hängt nicht nur von der technischen Umsetzung und Parametern wie der Redundanz ab, sondern ebenso davon, dass das Betriebspersonal möglichst keine Fehler macht. Deshalb definiert ITIL neben Prozessen auch Rollen und Aufgaben. Augenfällig wird dies in Unternehmen durch die Aufteilung von Aufgaben auf unterschiedliche Personen. So war es früher üblich, dass der für die Fehlerbehebung zuständige Techniker auch Upgrades einspielt und Konfigurationen entwickelt. Die strikte Trennung dieser Aufgaben erlaubt nicht nur eine Spezialisierung, sondern unterbindet auch Fehlerketten und etabliert ein Vieraugenprinzip.

ITIL ist kein Standard, sondern eine Sammlung von Empfehlungen, die an die konkreten Gegebenheiten innerhalb eines Providers anzupassen sind. Deshalb werden Zertifizierungen den geschulten und geprüften Mitarbeitern erteilt und nicht dem Unternehmen.

Man könnte ITIL als Esperanto für RZ-Betreiber bezeichnen; alle Wisenden verstehen genau das Gleiche unter Begriffen wie Change- und Problem-Management.

Allerdings sind die Wortschöpfungen teilweise etwas sperrig und setzen sich nur langsam in der Praxis durch. Eine Störung ist jetzt ein „Incident“ – die meisten Admins öffnen aber weiterhin einen „Case“ oder ein „(Trouble) Ticket“.

Mit der schnelllebigen IT-Welt ist auch ITIL einer ständigen Weiterentwicklung unterworfen. So bringt die im letzten Jahr veröffentlichte Version 4 größere Veränderungen (siehe iX 4/2019, S. 92) – auch als Reaktion auf Kritik an Komplexität und Aktualität der aus dem Jahr 2007 stammenden Vorgängerversion. In den Fokus rücken die Entwicklung neuer Services und die gesamte Wertschöpfungskette eines Serviceproviders. Außerdem werden Trends wie DevOps, Clouds und agile Softwareentwicklung berücksichtigt, die ganz neue Herausforderungen für das Management mit sich bringen.

Service-Management-Prozesse nach ITIL

Betrieb und Support Day-to-Day Operation

Incident Management
Problem Management
Change Management
Release Management
Configuration Management

Planung und Optimierung Long-Term Planning, Improvements

Service Level Management
Finanzen Management
Capacity Management
IT Continuity Management
Availability Management

ITIL unterscheidet zwischen operativen und strategischen Prozessen (Abb. 8).

Managed Services

Deutsche Hosting-Provider mit Managed Services

Hoster	Website	Produkte
1blu	www.1blu.de	Managed Hosting
3U TELECOM	www.3utelecom.de	Managed Cloud Services
Adacor	www.adacor.com	Managed Hosting, Managed Applications (Jira oder Confluence), Managed Cloud (AWS Cloud, Azure Cloud)
Anexia	www.anexia.com	Managed Server, Managed Cluster, Managed Database
bluechip	www.bluechip.de	Workplace as a Service
Boreus	www.boreus.de	Managed Hosting, Managed Cloud, Managed Security, Managed SAP
Bradler & Krantz	www.providerdienste.de	Managed Server für CMS und E-Commerce
centron	www.centron.de	Managed Server Dedicated/Virtual
Claranet	www.claranet.de	Managed Cloud Hosting, Managed Public Cloud, kundenindividuelle Managed Services
Continum	www.continum.net	Managed Hosting, Managed Kubernetes, Managed Cloud Services
Cronon	cronon.net	Managed Business Cloud, Managed Kubernetes, Managed VPN, Lizenzmanagement
cyberwebhosting.de	www.cyberwebhosting.de	Managed Server, Managed Virtual Server
Datagroup	www.datagroup.de	Application Management Services, Managed Cloud, u. a. Managed Active Directory, Robots as a Service, Managed LAN und WLAN
DM Solutions	www.dmsolutions.de	Managed Server
dogado	www.dogado.dewww.campusspeicher.de	Managed Server, Managed Firewall, Managed Storage, Managed Hosting, Managed AWS, Managed SharePoint, Managed Terminal Server, Managed Server, Managed Cloud
domainCAMP	www.railshosting.de	Managed Server für Ruby on Rails
domainfactory	www.df.eu	Managed Server
Droptop	linevast.de	Managed DevOps-Server (Docker, Jenkins, GitLab, MongoDB, Redis), Groupware-E-Mail, Ecommerce-Server
ebiz-consult	www.ebiz-webhosting.de	Managed Server
Everscale	www.everscale.de	Managed Server, Managed Cluster, Managed Services (CDN, DNS, Load Balancer), Managed Security
Filoo	www.filoo.de	Managed Jira und Confluence, Managed Load Balancing
First Colo	first-colo.net	Kubernetes as a Service, Managed Hosting
Fritz Managed IT	www.fritz.gmbh	Managed IT Services, Managed Cloud Services
GTT	www.gtt.net	Managed Network Services (einschließlich CPE), Managed Security
Herbst Datentechnik	www.herbst.de	Managed Hosting
Hetzner	www.hetzner.de	Managed Server
Host Europe	www.hosteurope.de	Monitoring, vServer-Administration, flexible Cluster-IP
hostNET	www.hostnet.de	Managed-Root Cloud, Dedicated Managed-Root Server
HostPress	www.hostpress.de	Managed WordPress Hosting
Hostserver	www.hostserver.de	Managed Hosting, Managed Server, Managed Cloud, AWS Managed Cloud
hosttech	www.hosttech.de	Managed Server
Hostway	www.hostway.de	Managed Backup / Firewall / Intrusion Detection / Load Balancing
Interares	www.intares.de	diverse Managed IT-Services
Inter.net	www.de.inter.net	Managed Service (Load Balancer, Georedundanz)
IONOS	www.ionos.de	Managed Kubernetes, Managed Cloud Hosting
ITENOS	www.itenos.de	Managed WAN
Leaseweb	www.leaseweb.com	Managed Cyber Security (SOC, SIEM, CERT)
managedhosting.de	www.managedhosting.de	IaaS, PaaS, Disaster Recovery as a Service, Microsoft Azure Stack
maxcluster	www.maxcluster.de	Managed Cluster, Managed Center
myLoc	www.myloc.de	Managed Server, Managed Storage, Managed Hosting (Cluster, E-Commerce), Microsoft Azure Stack
netcup	www.netcup.de	Managed Server, Managed Cloud Cluster
Netways	www.netways.de	Monitoring-Hardware, Automation (Puppet, Ansible), Management (GitLab, Kubernetes)
Noris Network	www.noris.cloud	OpenStack: Images as a Service, Alerts as a Service, Identity as a Service, Telemetry as a Service
PHP-Friends	php-friends.de	Managed Hosting
Plus.line	www.plusline.de	Managed Hosting
Plusnet	www.plusnet.de	Managed Network Services, MPLS VPN
PlusServer	www.plusserver.comwww.nimblu.com	Managed Kubernetes, Managed AWS, Managed Google Cloud, PlusCloud
Profihost	www.profihost.com	Managed Shop Hosting, Managed Cluster, Managed PIM Hosting
QualityHosting	www.qualityhosting.de	Managed Security 365 (MS Office)
Raidboxes	raidboxes.io	Managed WordPress Hosting
Riedel Networks	www.riedel-networks.net	Managed SD-WAN, Managed Ethernet
RobHost	www.robhost.de	Managed Server, Managed Cluster
root360	www.root360.de	AWS Managed Cloud Hosting, Managed Docker
ScaleUp	www.scaleuptech.com	Managed Hosting, Managed Kubernetes
sepago	www.sepago.de	Citrix Managed Services, Microsoft Cloud Managed Service, Managed Security Operations Center (Managed SOC)
Splendid Internet	www.splendid-internet.de	Managed Hosting für E-Commerce Magento, Shopware
Strato	www.strato.de	Managed Server, Managed Backup
TelemaxX	www.telemaxx.de	Managed Hosting (Server, Storage, Backup), Managed Cloud
Thomas-Krenn	www.filoo.de	Managed Jira und Confluence, Managed Load Balancing
Timme Hosting	timmehosting.de	Managed Server, Managed vServer (VPS)
Tralios	www.tralios.de	Managed Hosting, Managed Services, Managed Applications
Uptime	www.uptime.de	Managed Hosting
WebhostOne	www.webhostone.de	Managed Docker Server

In iX extra 4/2021: Hosting: Software as a Service

Die plötzliche Versetzung ganzer Abteilungen ins Homeoffice hat viele Unternehmen vor die Aufgabe gestellt, die Mitarbeiter mit VPN-Anschlüssen und Kommunikationswerkzeugen zu versorgen. So schlug die Stunde amerikanischer Cloud-Anbieter und vor dem eherne Grundsätze wie Datenschutz und Rechtssicherheit wurden zunächst weniger gründlich hinterfragt als notwendig. Inzwischen ist eine differenziertere Betrachtung angebracht. Da die Kommunikation zunehmend außerhalb der Unternehmensgrenzen

stattfindet und der Kontakt zu Partnern, Kunden und Lieferanten ohne Reisen umso wichtiger wird, ist es sinnvoll, Messenger, E-Mail-Konten, Voice- und Webkonferenzen nach Bedarf von spezialisierten Dienstleistern zu nutzen. Software-Services deutscher Hosting-Provider bieten dies mandantenfähig und nach heimischen Rechtsstandards. iX beleuchtet Markt und Möglichkeiten.

Erscheinungsdatum: 18.03.2021

Desktop, Asset Management, Service Desk) und realisieren auch eher kundenspezifische Projekte. Daneben spezialisieren sich einige ganz auf Dienstleistungen rund um eine Anwendung. Da im letzten halben Jahr Videokonferenzen zur neuen Dienstweise geworden sind, sei hier stellvertretend die Video- und Medientechnik genannt (PIK AG).

Die Folgen der Coronapandemie bekommen IT-Dienstleister aber auch in negativer Hinsicht zu spüren. Bei einigen Systemhäusern gibt es Kurzarbeit. Laut der Information Services Group (ISG) ist der weltweite Umsatz mit Managed Services allein im zweiten Quartal um 17% eingebrochen, da Fabriken und Lieferketten stillstehen. Infrastructure as a Service hingegen verzeichnete im gleichen Zeitraum dank Homeoffice und E-Learning einen spürbaren Umsatzanstieg. Da die Digitalisierung vor allem in der öffentlichen Verwaltung, im Gesundheits- und Bildungswesen in den letzten Monaten im Zeitraffer vorangeschritten ist, haben die Anbieter von Netzwerk- und RZ-Services alle Chancen, zu den Gewinnern der gegenwärtigen Veränderungen zu gehören. (un@ix.de)

Uwe Schulze
ist freier Autor in Berlin.

Die weiteren iX extras

Ausgabe	Thema	Erscheinungsdatum
5/2021	Security: Managed Security Services für KMU	22.04.2021
6/2021	Storage: Neue Storage-Technik	27.05.2021
7/2021	Cloud-Computing: Public Cloud made in Germany	24.06.2021

Beispiel ist Raidboxes mit allen Services rund um WordPress.

Die meisten Angebote für Managed Applications gibt es aus den Bereichen Groupware, Content-Management-Systeme (CMS) und E-Commerce. Während hier Open-Source-Software vorherrscht, gibt es entsprechende Leistungen auch für kommerzielle Softwarepakete, etwa Managed SAP. Es müssen aber nicht die großen Anwendungen sein, die ein Provider betreibt; möglich sind auch ein-

zelne Funktionen. So bietet Intares Managed Mailrelay und Managed Mailfiltering als Dienst an. Entwickler werden bei Linux fündig, wo es Managed DevOps (Docker, Git, Ruby und Node.js) als Service gibt.

Service mit System

Nicht nur Hosting-Provider, sondern auch klassische IT-Systemhäuser und Integrierten erweitern ihr Produktportfolio

zunehmend um Managed Services. Ihr Geschäftsmodell entstammt ursprünglich dem Handel mit Hardware und Software, der bedingt durch sinkende Margen mehr und mehr um Dienstleistungen angereichert wurde. Managed Services sollen dabei helfen, diese standardisiert und günstig zu produzieren und Kunden über einzelne Projekte hinaus zu binden. Große IT-Systemhäuser mit breitem Angebot bieten vor allem Services außerhalb des Hostings an (Managed