Whitepaper

Secure Remote Services

Public Cloud vs. Private Cloud (On-Premise)

Erfahren Sie mehr über

- Die wichtigsten Unterschiede
- Vorteile für Ihr Unternehmen
- Risiken im Setup und Betrieb

PHOENIX CONTACT

Einleitung

Die immer größere Bedeutung von Public-Cloud-Lösungen bewegt viele Anbieter von Remote-Service-Lösungen dazu, ihren Fokus von On-Premise-Lösungen hin zu cloud-basierten Bereitstellungsmodellen zu verschieben. Mit diesem Wandel stellt sich eine entscheidende Frage: „Welche Lösung ist für mein Geschäft am besten geeignet?“ Wenn Sie sich fragen, welche Option sich mit Blick auf Sicherheit, Zugänglichkeit und Erschwinglichkeit empfiehlt, erhalten Sie in diesem Whitepaper die Antworten auf Ihre Fragen.

Die Landschaft der Cloud Managed Services wird immer anspruchsvoller und wettbewerbsfähiger laut einer Gartner-Studie*.
Tatsächlich werden 2022 bis zu 60 % der Unternehmen das Public-Cloud-Service-Angebot eines externen Dienstleisters nutzen, was einer Verdopplung des Prozentsatzes der Unternehmen von 2018 und einem Volumen von 354.6 Milliarden USD entspricht.
Die Vorteile der Cloud liegen klar auf der Hand: Sie bietet nicht nur mehr Agilität und stets aktuelle Software, sondern beseitigt auch hardwareseitige Einschränkungen. Überraschenderweise werden die Vor- und Nachteile von Cloud- und On-Premise-Software weiterhin intensiv diskutiert.

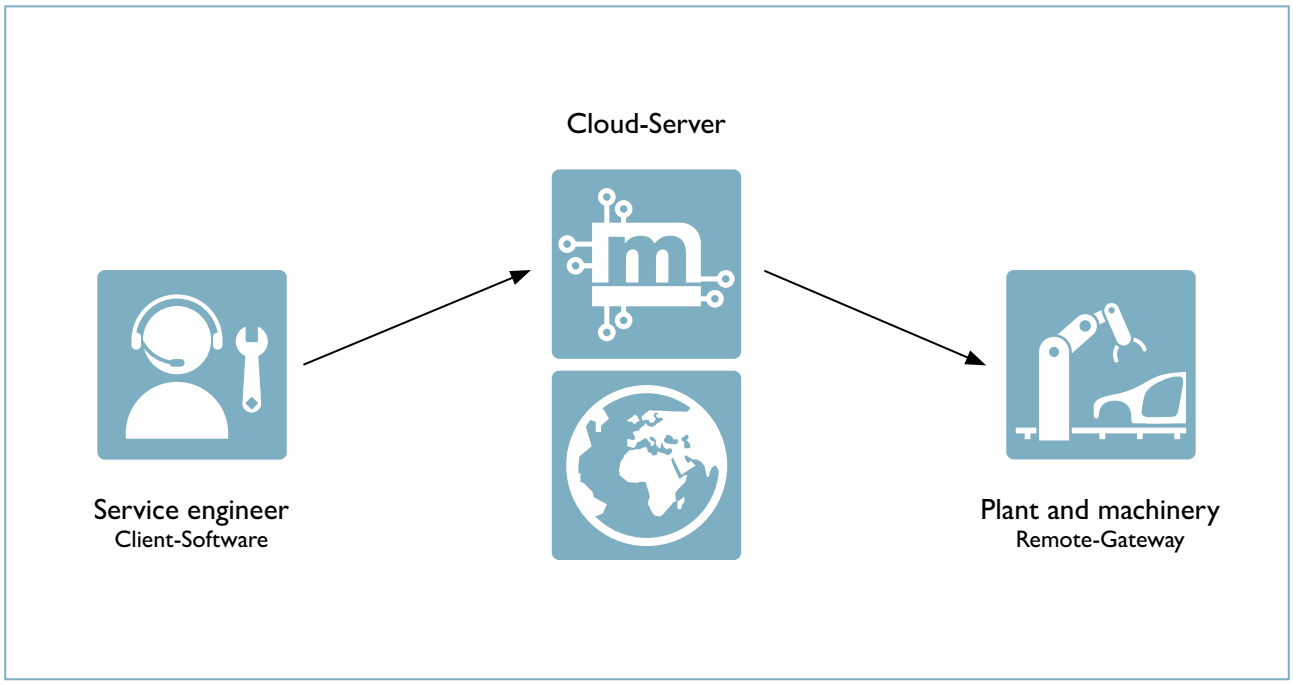
* Quelle: Gartner, November 2019
https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020

Der Hauptunterschied zwischen Cloud- und On-Premise-Software besteht im Wesentlichen in ihrem Installationsort. On-Premise-Software wird lokal auf den Computern und Servern Ihres Unternehmens installiert, während Cloud-Software in der Serverfarm eines Anbieters gehostet und betrieben und über einen Webbrowser genutzt wird.

Neben der Zugänglichkeit müssen natürlich noch weitere Faktoren im Entscheidungsprozess berücksichtigt werden: Software-Eigentum, Betriebskosten, Software-Updates, Backup-Strategie und zusätzliche Services wie Sicherheit, Support und Implementierung. Im Folgenden sollen nun die Vor- und Nachteile besprochen werden.

Inhalt

1 Grundlagenwissen zur Cloud



Typische Remote-Services-Cloud-Topologie

Beim cloudbasierten Fernzugriff handelt es sich um eine neue Art von sicherem Remote Service, der flexiblen Fernzugriff auf die Maschinen im Feld ermöglicht.

Die zugehörige Netzwerktopologie besteht aus drei Komponenten:

1. Remote-Gateway
Remote-Gateways stellen für Zugriff und Steuerung eine Verbindung mit den Betriebsmitteln im Feld her.

2. Cloud-Server
Der Cloud-Server ist auf einer cloudbasierten Plattform wie Amazon Web Services oder Microsoft Azure installiert. Er ordnet die Verbindungsanfragen zu und stellt nach erfolgreicher Authentifizierung auf beiden Seiten eine Verbindung her.

3. Client-Software
Die Client-Software wird auf dem Mobilgerät, PC oder Desktop des Technikers installiert. Remote-Gateway und Client-Software initiieren ausgehende sichere Verbindungsanfragen an den Cloud-Server.

2 Vorteile der Cloud

Cloudbasierte Fernzugriffslösungen implementieren Netzwerktopologien, mit denen ausgehende Verbindungen in Form von Fernzugriffstunneln ermöglicht werden. Dadurch können die Herausforderungen bewältigt werden, die sich bei herkömmlichen VPN- und Remote-Desktop-Steuerungstechniken stellen.

Außerdem bietet cloudbasierter Fernzugriff den Maschinenherstellern die folgenden Vorteile:

Benutzerfreundlichkeit

Für den Fernzugriff über Plug-and-Play ist keine technische Konfiguration mehr erforderlich. Sicherheitsparameter wie Hash-Funktionen und Algorithmen für Ver- und Entschlüsselung werden automatisch konfiguriert. Maschinenhersteller müssen diese Parameter nicht konfigurieren, sondern können eine Remote-Verbindung einfach per Mausklick herstellen.

Dank virtueller IP-Adressen ist der Mehrpunktzugriff mühelos und ohne IP-Neukonfiguration vor Ort möglich. Unabhängig von den anfänglichen IP-Adressen, die durch die Maschinenhersteller eingerichtet wurden, weist die cloudbasierte Software den Maschinen eindeutige virtuelle IP-Adressen zu. Die Maschinenhersteller können mithilfe dieser virtuellen IP-Adressen mehrere gleichzeitige Remote-Verbindungen herstellen. Außerdem können Maschinenhersteller identische IP-Schemata für verschiedene Standorte verwenden, ohne sich über Adresskonflikte Gedanken machen zu müssen. Dies wiederum trägt zu einer beträchtlichen Reduzierung der Kosten für die Installation bei.

Die Verbindungen werden zentral überwacht und verwaltet. Der Cloud-Server ist der zentrale Punkt, um Remote-Verbindungen herzustellen und zu verwalten. Administratoren können sich mit dem Cloud-Server verbinden, um Status und Volumen des Datenverkehrs jeder Verbindung zu überwachen. Außerdem können Administratoren auf einfache Weise Client-Konten, Remote-Gateways und Zertifikate verwalten, ohne sie regelmäßig neu konfigurieren zu müssen.

Erweiterte Sicherheit

Die End-to-End-Verschlüsselung zwischen einem Remote-PC und einem Betriebsmittel verhindert Datenlecks. Der Cloud-Server leitet den Datenverkehr lediglich weiter: Die durchgeleiteten Daten werden weder entschlüsselt noch gespeichert.

Maschinenhersteller verwenden Fernzugriff für Fehlerbehebung, Überwachung, Wartung und Diagnose. Der Fernzugriff ist typischerweise nicht kontinuierlich nötig, so dass es ausreicht, ihn bei Bedarf zu verwenden. Dies trägt zur Minimierung von Sicherheitsproblemen und zur Kostenreduzierung bei – insbesondere, wenn die Remote-Konnektivität volumenbasiert abgerechnet wird, wie es bei Mobilfunktechnologie üblich ist.

Außerdem ziehen die Maschinenbetreiber den Fernzugriff der Maschinenhersteller auf alle Anwendungen in ihrem lokalen Netzwerk vor. Wenn der Zugriff auf die Anwendungen beschränkt wird, die die Maschinenhersteller benötigen, wird das Risiko einer möglichen Beeinträchtigung der Betriebsabläufe beseitigt. Cloudbasierter Zugriff ermöglicht es Maschinenbetreibern, Remote-Verbindungen zu initiieren oder zu akzeptieren. Außerdem können Maschinenbetreiber Regeln zu den Services und

Anwendungen festlegen, die Maschinenhersteller remote verwenden können. Sie können auch den Zugriff auf bestimmte Gruppen von Servicetechnikern beschränken.

IT-Sicherheitsrichtlinien werden kompromisslos befolgt. Cloudbasierte Fernzugriffslösungen können ausgehende Verbindungen mithilfe der IPsec VPN-Ports 4500 und 500 herstellen, das heißt, dass diese Ports für VPN-Datenverkehr geöffnet werden. Dadurch entstehen jedoch gleichzeitig Probleme mit IT- und Firewall-Managern. Wird hierfür jedoch der Firewall-freundliche Service-Port 443 (für sicheren Website-Zugriff mithilfe von SSL) oder 80 (für ungesicherten Website-Zugriff) für den Remote-Zugriff verwendet, entstehen keinerlei Probleme für die verwaltenden IT-Abteilungen.
Diese Lösung kann laut IT-Sicherheitsrichtlinien der Maschinenbetreiber bedenkenlos genutzt werden.

Flexibilität und Skalierbarkeit

Die Client-Software ist nicht auf spezifische Hardware-Plattformen beschränkt. Die Benutzer können Client-Software auf beliebige Mobilgeräte, Laptops oder PCs herunterladen, um dann jederzeit von beliebigen Orten aus den Fernzugriff zu nutzen, sofern sie über ein aktives Client-Konto verfügen.

Mit dem Fernzugriff auf Betriebsmittel stehen den Benutzern dieselben Möglichkeiten wie bei einer lokalen Verbindung zur Verfügung. Durch die Verbindung zwischen Client und Remote-Betriebsmitteln über einen transparenten Tunnel gibt es keine Unterschiede mehr gegenüber einer Platzierung im selben Netzwerk. Unabhängig von den Remote-Betriebsmitteln, auf die zugegriffen wird (SPS, HMI usw.), und ungeachtet des verwendeten Protokolls für Datenabruf oder Programmierung können Maschinenhersteller Remote-Daten erfassen oder (Remote)-Betriebsmittel programmieren. Zu diesem Zweck können sie ihre eigenen Software-Tools auf dieselbe Weise wie beim Arbeiten direkt an den Betriebsmitteln verwenden.

Der Fernzugriff erleichtert die Erweiterung von Netzwerken, da Netzwerkadministratoren problemlos Betriebsmittel hinzufügen und entfernen und Client-Konten und -Zertifikate verwalten können.

OEMs und Maschinenhersteller benötigen sicheren, benutzerfreundlichen und skalierbaren On-Demand-Fernzugriff auf ihre Maschinen im Feld.

Herkömmliche On-Premise-Zugriffslösungen sind umständlich und erfordern Kenntnisse über IT-/Netzwerktechnologie sowie Änderungen an den Sicherheits-/Firewall-Richtlinien.

Wenn der Fernzugriff durch eine cloudbasierte Management-Infrastruktur unterstützt wird, erhalten die OEMs das erforderliche hohe Maß an Benutzerfreundlichkeit, Flexibilität und Skalierbarkeit, ohne dass die Sicherheit dadurch beeinträchtigt wird.

3 Kosten

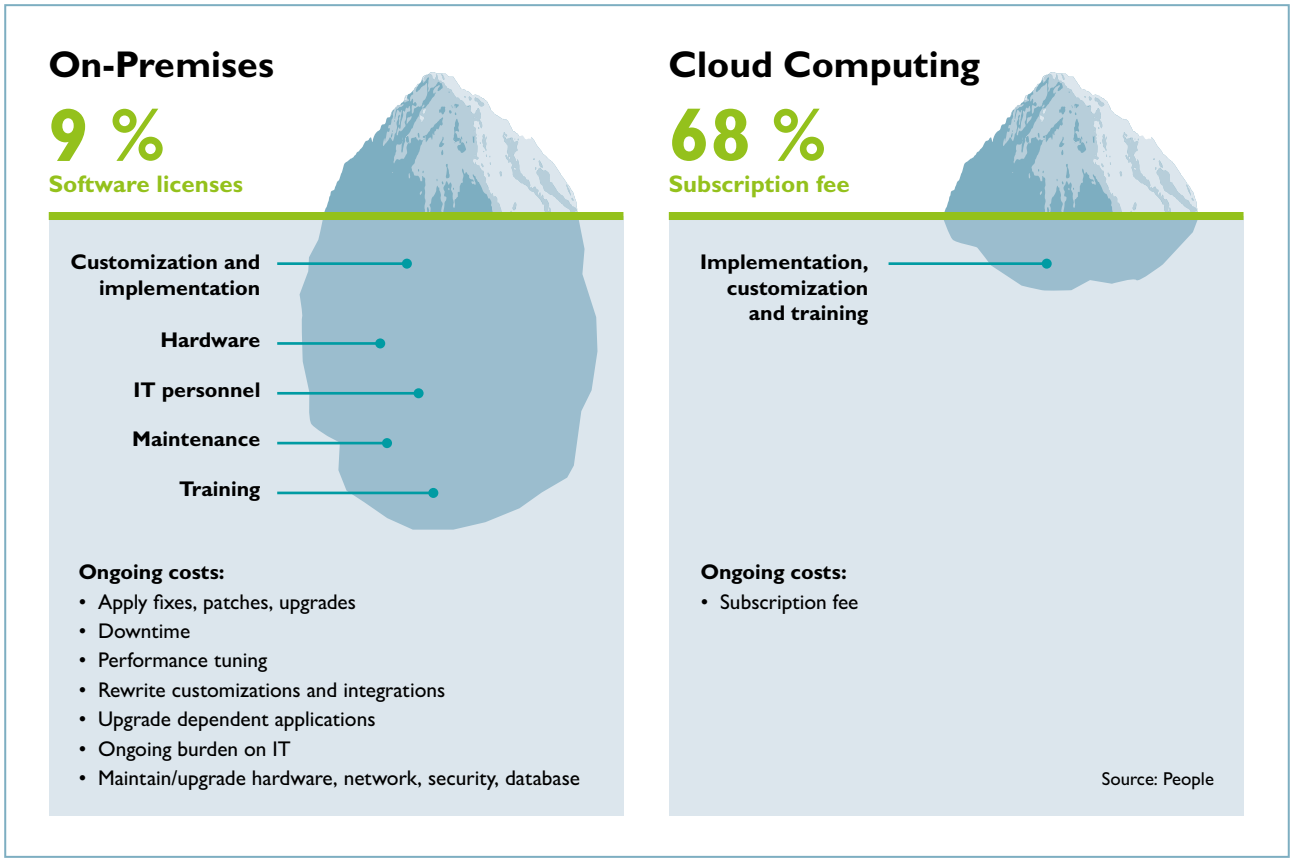
Ähnlich wie bei einem Eisberg, bei dem das meiste verborgen ist, sind auch die Kostenvorteile einer cloudbasierten Lösung nicht auf Anhieb ersichtlich. Beginnen wir mit den Teilen, die Sie sehen können:

- **Initialkosten**
- **Abonnements**
- **Software-Lizenzen**

Mit einer On-Premise-Lösung werden Ihre Kosten für die Einrichtung höchstwahrscheinlich sehr viel höher. Allein aus diesem Grund sind Sie mit einer Cloud-Lösung besser bedient, wenn Sie keine höheren Summen investieren möchten: Sie bezahlen einfach pro Monat/Quartal/Jahr eine Abogebühr, anstatt die Software zu kaufen.

Diese monatliche Abogebühr ist fast teurer als die laufenden Lizenzgebühren für die von Ihnen gekaufte Software – in dieser Hinsicht ist eine On-Premise-Lösung also langfristig kostengünstiger.

Allerdings ist der Vergleich damit noch nicht beendet – On-Premise-Lösungen bringen eine Vielzahl verborgener Kosten mit sich, die nicht klar ausgewiesen werden. Sofern Sie nicht in der Lage sind, diese Kosten durch sehr effiziente Verfahren unter Kontrolle zu halten, zahlen Sie normalerweise mit einer On-Premise-Lösung wesentlich mehr als für eine gehostete Cloud-Lösung.



Kostenvorteile Cloud-basierter Lösungen: Sichtbare und verdeckte Kosten

4 Risiken durch On-Premise-Lösungen

Mit einer Private Cloud in Ihrem On-Premise-Rechenzentrum werden die Karten möglicherweise neu gemischt. „Private Cloud“ bedeutet, dass Sie die volle Leistung von On-Demand-Computing nutzen können, aber gleichzeitig so flexibel sind, um eine maßgeschneiderte technische Lösung zu realisieren. Mit einer Private Cloud sind Sie nicht mehr von Anbietern wie Amazon Web Services (AWS) und Microsoft Azure abhängig, sondern können Ihre Vorstellungen umsetzen. So ist es beispielsweise möglich, Daten lokal zu speichern und die Compliance-Anforderungen problemlos zu erfüllen. In vielen Fällen ermöglicht diese Methode zudem beträchtliche Kosteneinsparungen.

Allerdings bringen Private Clouds ihre ganz speziellen Herausforderungen mit sich. Mit der Einführung einer Private Cloud wird Ihre Organisation mehreren und teilweise weitgehend unbekannten Risiken ausgesetzt. Wie lauten diese Risiken und wie könnten sie Ihre Entscheidung für eine Private oder Public Cloud beeinflussen? Letztlich ist auch eine Private Cloud weiterhin eine Cloud.

Risiko Nr. 1: Sicherheitsverletzungen

Private Clouds sind möglicherweise unsicherer als Public Clouds. Die Anbieter von Public Clouds verfügen über jahrelange Erfahrung und erstklassiges Know-how in Sicherheitsfragen. In vielen Fällen können sie daher auf Strategien, Techniken und Tools zurückgreifen, um die verschiedenen Ebenen des Cloud-Stacks abzusichern. Es ist sicherlich richtig, dass Public Clouds für Hacker ein größeres Angriffsziel darstellen. Allerdings kennen die Cloud-Anbieter nicht nur die potenziellen Sicherheitsprobleme von Clouds, sondern auch die entsprechenden Gegenmaßnahmen, was Sie als privates Unternehmen erst noch lernen müssen.

Auch Hybrid Clouds können problematisch sein. Die Sicherheit in einer Hybrid Cloud ist sogar noch komplexer. Wenn Sie die anfallenden Arbeiten von der Private in die Public Cloud verschieben, dann werden auch Ihre internen Sicherheitssysteme durch die Systeme ersetzt, die in der Public Cloud angeboten werden. Während dieses Übergangs, wenn Datenverkehr und Apps von einem System zum anderen wechseln, besteht ein beträchtliches Risiko von Sicherheitslücken, die zu Missbrauch einladen.

Risiko Nr. 2: Leistung

Leistung ist ein altbekanntes Problem von virtualisierten Umgebungen. Aufgrund der hochgradig dynamischen Natur der Umgebung kann nur schwerlich vorhergesagt werden, wie sich schwankende Belastungen auf Infrastrukturebene auf Anwendungsleistung und Benutzererfahrung auswirken.
Die Unternehmen kennen zwar ihre Computing-Ressourcen und die Anzahl von Rechnerinstanzen in der Public Cloud, aber es gibt weitere leistungsrelevante Faktoren – Netzwerkbandbreite, Latenz und Schwankungen, potenziell störende Nachbarn in gemeinsam genutzten Computing-Ressourcen, Zugriffsgeschwindigkeit und mehr.

Die Private Cloud kann viel flexibler gestaltet werden. Sie können die Hardware- und Software-Komponenten, Netzwerkinfrastruktur und Topologie auswählen, die Ihrer Meinung nach die optimale Leistung für Ihren Anwendungsfall ermöglichen. Aber erzielen Sie damit wirklich die erwartete Leistung?

Genauso, wie Anbieter von Public Clouds aufgrund der Komplexität von virtualisierten und sich dynamisch ändernden Infrastrukturen ihren Benutzern nicht immer die benötigte Leistung bereitstellen können, **werden Sie auch mit einer Private Cloud nicht immer Ihre angestrebte Leistung erreichen.**

In virtualisierten Systemen können verborgene Engpässe auftreten. Die Leistung könnte je nach aktueller Mischung aus Arbeitslast, Software-Upgrades von VMware, OpenStack oder anderen Systemelementen und vielen anderen Faktoren variieren. Sind Sie sicher, dass Ihre Infrastruktur bei allen Anwendungsfällen und Umgebungsbedingungen Ihre gewünschte Leistung erbringt? Und dass das auch bei Upgrades so bleibt?

Risiko Nr. 3: Know-how und Lernkurve

Private Clouds gibt es schon seit einiger Zeit und viele wurden mithilfe der bestens bekannten und verbreiteten VMware Software-Infrastruktur erstellt. Allerdings entscheiden sich immer mehr Private Cloud-Projekte für die leistungsfähige und kostengünstigere Option einer Open Source-Plattform. OpenStack zeichnet sich de facto als neuer Standard für Private Clouds ab, aber diese Plattform bringt viele Unwägbarkeiten mit sich.

Wenn Sie keine versierten Experten für OpenStack in Ihrem Team haben (von denen es nicht besonders viele gibt), dann sind die ersten Schritte mit einem OpenStack-Projekt eine extreme Herausforderung. In der Benutzerumfrage zu OpenStack aus dem Jahr 2016 äußerten sich Benutzer zur Schwierigkeit und Komplexität beim Arbeiten mit OpenStack, obwohl die Plattform ausgereifter wird.

Wenn Sie bei einer Bereitstellung von OpenStack nicht von Anfang an alles richtig machen, könnten Sie später in große Schwierigkeiten geraten. Dadurch sind Sie möglicherweise nicht mehr in der Lage, die Private Cloud mit genau den benötigten Fähigkeiten zu erstellen und die Meilensteine Ihres Projekts einzuhalten.

Risiko Nr. 4: Fehlende Einblicke

Einer der Gründe für den Wechsel von der Public in die Private Cloud besteht darin, zusätzliche Einblicke in die Abläufe in der Cloud zu gewinnen. **Häufig wird die Meinung vertreten, dass Sie viel bessere Einblicke in Faktoren wie Arbeitslasten, Nutzung, Datenverkehr und Leistung haben, sobald etwas in Ihrem eigenen Rechenzentrum betrieben wird.**

In der Public Cloud existiert keine einfache Lösung, um Einblicke in Ihren Netzwerkdatenverkehr auf Paketebene zu erhalten. Mit vorhandenen Überwachungstools wie CloudWatch und CloudTrail von Amazon können Sie die Pakete nicht näher inspizieren, um eine umfassendere Diagnose von Netzwerkproblemen ausführen und Sicherheitsprobleme verhindern zu können.

In der Private Cloud ist die Situation nicht viel besser. Sie werden mit dem Problem konfrontiert, dass Netzwerkdatenverkehr zwischen virtuellen Rechnern (VMs) ohne physikalische Übertragungswege fließt und somit für die herkömmlichen Überwachungstools völlig unsichtbar ist. **Dieser Datenverkehr kann 80 % oder mehr des Datenverkehrs in einem virtualisierten Rechenzentrum ausmachen, sodass eine große Unbekannte für die IT-Teams entsteht.**

Risiko Nr. 5: Begrenzter Umfang

Viele Unternehmen ersetzen ihr herkömmliches Rechenzentrum durch eine Private Cloud, um die Leistung von On-Demand-Computing nutzen und Unternehmensanwendungen und -services schneller entwickeln zu können. Allerdings wird die Kapazität Ihrer Private Cloud letztlich durch Ihr Budget begrenzt.

Was geschieht, wenn die Anwendungsnutzung Ihre Erwartungen deutlich übertrifft? Angenommen, Sie bieten Ihren Kunden einen Service an, dessen Nutzung explosionsartig steigt, wie kann Ihre Cloud dies unterstützen? Sie setzen sich dem Risiko aus, Ihre Kapazität zu überschreiten und somit die Skaleneffekte und Kosteneinsparungen zu verlieren, die der Hauptgrund für das Erstellen Ihrer Private Cloud waren.

Die klassische Lösung für dieses Problem ist eine Hybrid Cloud, mit der Aufgaben von der Private Cloud in die Public Cloud verlagert werden, falls Arbeitslasten Ihre lokalen Ressourcen überfordern. Aber die Einrichtung einer Hybrid Cloud führt zu mehr Kosten und Komplexität für Ihr Private-Cloud-Projekt. Außerdem ist die Einhaltung interner Richtlinien oder externer Vorschriften einer der gängigsten und wichtigsten Gründe für die Erstellung einer Private Cloud.

Es könnte eine interne Richtlinie existieren, laut der hochgradig vertrauliche Daten vor Ort gespeichert werden müssen und nicht in die Public Cloud verlagert werden dürfen, oder eine gesetzliche Vorschrift, dass Daten nicht das Land verlassen dürfen. Die Verwendung einer Hybrid Cloud für Lastspitzen in diesen Szenarien könnte problematisch sein. Aber wie können Sie sicherstellen, dass Load Balancing zwischen Private und Public Clouds nur für nicht vertrauliche Arbeitsumfänge erfolgt, während vertrauliche oder Vorschriften unterliegende Daten in Ihren Einrichtungen verbleiben?

Risiko Nr. 6: Eingeschränkte Services

Dies gilt nicht nur für den Umfang oder die Cloud-Services und -Fähigkeiten. In einer Public Cloud wie Amazon Web Services oder Microsoft Azure haben Sie Zugriff auf eine unglaubliche Vielzahl von Cloud-Services, ob nativ oder von Drittanbietern. Sie sind nur einen Mausklick entfernt und decken alle Anforderungen ab: von erweiterten Management-Fähigkeiten zu automatischer Skalierung und hoher Verfügbarkeit, Speicherdiensten, sofortiger Bereitstellung von Datenbanken und großen Datenclustern usw.

Auch wenn Sie die meisten dieser Fähigkeiten in der Private Cloud nutzen können, müssen Sie diese einplanen und dann Geld und Zeit für Integration und Bereitstellung dieser Features aufwenden. In manchen Fällen müssen Sie Fähigkeiten sogar von Grund auf neu erstellen.

Insbesondere hohe Verfügbarkeit und Resilienzfunktionen, die durch Cloud-Services wie Amazon AWS bereitgestellt werden, können firmenintern nur schwer nachgebildet werden. Ein Feature wie mehrfache Availability Zones, mit dem Sie Rechnerinstanzen in verschiedenen Rechenzentren replizieren können, ist in den meisten Private Clouds nicht möglich.

Die **Quintessenz** ist, dass Ihnen **in einer Private Cloud nur die Funktionen zur Verfügung stehen, die Sie selbst erstellt haben.** Wenn Sie bestimmte Features, Funktionalitäten oder regelmäßige Updates nicht in Ihren Projektumfang aufgenommen haben, schränkt dies Ihre Innovationsfähigkeit in der Private Cloud ein.

Risiko Nr. 7: Datenverlust

Laut Daten von Veritas* sind viele Private-Cloud-Implementierungen größeren Risiken von Datenverlust ausgesetzt. Datenverluste können auf drei Ebenen auftreten: auf der Ebene von Hypervisor, virtuellem Rechner und Notfallwiederherstellung oder Backup-System.

Aufgrund der dynamischen Natur einer Private Cloud sind herkömmliche Technologien für den Schutz der Daten möglicherweise nicht ausreichend und funktionieren unter Umständen auch nicht in allen Szenarien auf vorhersehbare Weise. Es gibt auch zahlreiche Szenarien mit Fehlkonfigurationen, die verheerende Folgen haben können.

Wenn mehrere Versionen von VMware ESX ausgeführt werden, von denen einige die VMFS-Optionen (Virtual Machine File System) nutzen, die von früheren Versionen nicht unterstützt werden, kann dies zu Störungen an einigen VMs, zu Datenverlust und Ausfallzeiten führen.

Wenn eine kritische Anwendung auf zwei VMs mit einer Live-Kopie und einer Sicherungskopie läuft, dann wird beim Ausfall einer dieser VMs typischerweise ein automatisches Failover ausgeführt. Falls dieses Failover das Backup auf demselben physischen Host wie die Live-Kopie instanziiert, gibt es einen Single Point of Failure.

Wenn ein Hochleistungs-RAID 1 für Produktionsdaten und ein leistungsschwächeres RAID 5 für Archivierung und Zwischenspeicherung existiert, könnte es zu einer Diskrepanz kommen. Dies führt dazu, dass manche VMs Produktionsdaten auf den leistungsschwächeren Speicher schreiben, was Leistungseinbußen oder Datenverlust verursachen könnte.

* https://www.veritas.com/information-center/enterprise-cloud-storage-ultimate-guide

5 Pro und Contra von Public Cloud vs. Private Cloud (On-Premise)

Vorteile der Cloud-Software

Jederzeit Zugriff von überall
Sie können auf Ihre Anwendungen jederzeit und zu einem beliebigen Zeitpunkt über einen Webbrowser von einem beliebigen Gerät aus zugreifen.

Erschwinglich
Für die Cloud fallen vorab keine Kosten an. Sie nehmen stattdessen regelmäßige Zahlungen vor, so dass es sich um eine Betriebsausgabe (OpEx) handelt. Auch wenn sich die monatlichen Kosten im Lauf der Zeit aufsummieren, sind Wartungs- und Supportservices enthalten, was jährliche Verträge überflüssig macht.

Vorhersehbare Kosten
Profitieren Sie von vorhersehbaren monatlichen Zahlungen, die Software-Lizenzen, Upgrades, Support und tägliche Sicherungen abdecken.

Sorgenfreie IT
Weil Cloud-Software für Sie gehostet wird, müssen Sie sich keine Sorgen über die Wartung Ihrer Software oder die zugehörige Hardware machen, Kompatibilität und Updates werden durch den Cloud-Dienstanbieter übernommen.

Hohe Sicherheitsniveaus
Rechenzentren setzen Sicherheitsmaßnahmen ein, die über das hinausgehen, was sich die meisten Unternehmen leisten können. Daher sind Ihre Daten häufig in der Cloud sicherer als auf einem Server in Ihren Büros.

Schnelle Bereitstellung
Die Bereitstellung von cloudbasierter Software über das Internet ist im Gegensatz zu On-Premise-Anwendungen eine Sache von Stunden oder Tagen, da letztere auf einem physikalischen Server und jedem PC oder Laptop installiert werden müssen.

Skalierbarkeit
Cloud-Technologien ermöglichen größere Flexibilität, da Sie nur für Ihre tatsächliche Nutzung zahlen. Außerdem kann sie problemlos skaliert werden, um die jeweilige Nachfrage zu erfüllen, beispielsweise durch das Hinzufügen oder Reduzieren von Lizenzen.

Niedrigere Energiekosten
Wenn Sie in die Cloud wechseln, müssen Sie nicht mehr den Energieverbrauch Ihrer On-Premise-Server bezahlen oder das passende Umfeld für Ihre Server schaffen. Dadurch sinken Ihre Energiekosten beträchtlich.

Nachteile der Cloud-Software

Konnektivität
Für Cloud-Lösungen ist ein zuverlässiger Internetzugriff erforderlich, damit Sie produktiv bleiben.

Langfristige Kosten
Obwohl die Investitionen im Vorfeld niedriger sind, können Cloud-Anwendungen im Lebenszyklus des Systems insgesamt kostspieliger sein, was die Gesamtbetriebskosten (TCO) erhöht.

Weniger anpassbar
Cloud-Software ist typischerweise konfigurierbar, aber je nach Hosting könnte eine Cloud-Lösung möglicherweise komplexen Entwicklungsprojekten nicht gewachsen sein.

Vorteile von On-Premise-Lösungen

Gesamtbetriebskosten
Da Sie nur einmal für Ihre Benutzerlizenzen zahlen, kann eine On-Premise-Lösung unter Umständen geringere Gesamtbetriebskosten (TCO) als ein Cloud-System haben.

Komplette Kontrolle
Ob Daten, Hardware- oder Software-Plattformen: Alles gehört Ihnen. Sie entscheiden selbst über die Konfiguration, die Upgrades und Systemänderungen.

Betriebszeit
Mit On-Premise-Systemen müssen Sie sich nicht auf Internetkonnektivität oder äußere Einflüsse für den Zugriff auf Ihre Software verlassen.

Nachteile von On-Premise-Lösungen

Große Kapitalausgabe
Für On-Premise-Systeme ist üblicherweise ein hoher Kaufpreis vorab zu entrichten, so dass oft Kapitalausgaben (CapEx) erforderlich sind. Zudem müssen Sie noch die Wartungskosten einrechnen, um Support und Upgrades für die Funktionalität zu gewährleisten.

Verantwortlichkeit für die Wartung
Bei einem On-Premise-System sind Sie dafür verantwortlich, die Server-Hardware und -Software zu warten, und müssen sich um Sicherheitsprobleme, Datensicherungen, Speicherung und Notfallwiederherstellung kümmern. Dies kann ein Problem für kleinere Unternehmen darstellen, die begrenzte Budgets und technische IT-Ressourcen haben.

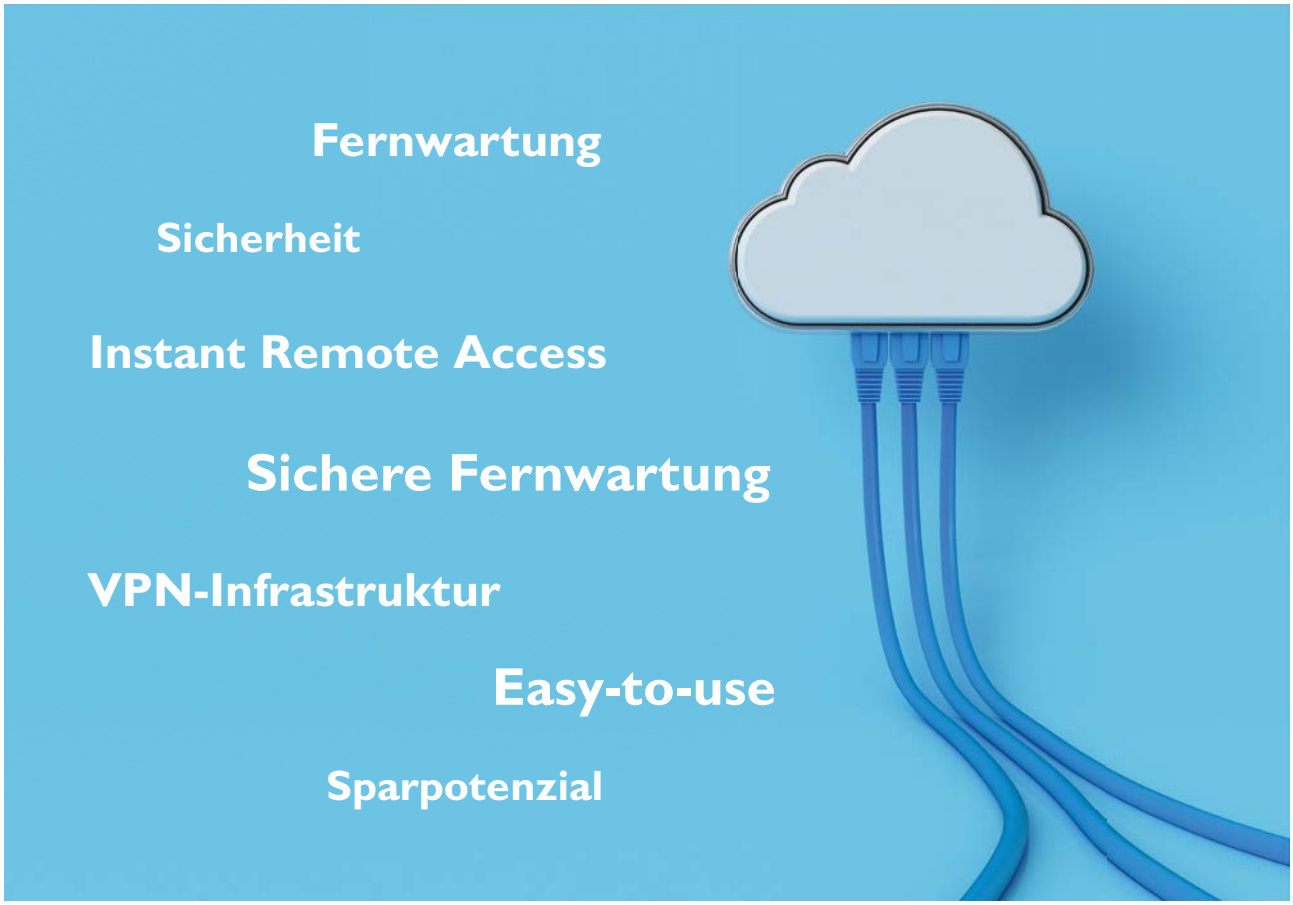
Längere Implementierungsdauer
Die On-Premise-Implementierung dauert länger, da Zeit für die Installation auf den Servern und jedem einzelnen Computer oder Laptop erforderlich ist.

6 Fazit

Warum sind cloudbasierte Remote Services besser als On-Premise-Lösungen?

Cloud-Lösungen sind nicht nur aufgrund ihrer Flexibilität, Zuverlässigkeit und Sicherheit besser als On-Premise-Lösungen. Sie ersparen Ihnen auch noch den Aufwand für Wartung und Aktualisierung Ihrer Systeme. Dadurch können Sie Ihr Geld, Ihre Zeit und Ihre Ressourcen in die Umsetzung der Strategien für Ihr Kerngeschäft investieren.

Aufgrund der Bereitstellung von standortunabhängigem Echtzeitzugriff auf Systeme und Daten von einer Vielzahl von Geräten und einer garantierten Betriebszeit von 99 % wird die Cloud zur ersten Wahl für alle Unternehmen, die Remote Services nutzen.



Kontakt

Secure Remote Services

Als strategischer Produktmanager suche ich stets nach den besten und nicht den einfachsten Antworten für Technologie, Design, Benutzererfahrung und Geschwindigkeit.
Das Ergebnis sind nachhaltige und herausragende Produkte, die Ihnen den Weg für den flexiblen Zugriff auf Ihre Maschinen und Anlagen im Feld ebnen.

Finden Sie die optimale Remote-Service-Lösung für Ihr Unternehmen und sichern Sie sich einen Beratungstermin.

https://phoe.co/mGuardSecureRemoteService

Markus Scheibenpflug
Strategischer Produktmanager
Communication Interfaces
Automation Infrastructure bei
Phoenix Contact

mscheibenpflug@phoenixcontact.com

AI 03-21.006.L3