01.09.2019 / cr

Die perfekte Cloud-Umgebung erzeugt den perfekten Kopfschmerz für den Datenschutz

Wer mich kennt weiß, daß ich vom **Backup in die Cloud** absolut gar nichts halte:

- Beim Backup in eine **private Cloud** fügen Sie eine zusätzliche Ebene in Ihr Backup-Konzept ein, die überhaupt nicht notwendig ist.
  Hierdurch verursachen Sie nur zusätzliche Kosten und erhöhen den administrativen Aufwand erheblich.

- Beim Backup in eine **public Cloud** geben Sie Ihre wervollen Daten außer Haus. Damit allerdings geben Sie bereits eine wesentliche Grundlage der Datensicherheit auf.
  Zum Glück jedoch verhindert die in Deutschland zur Verfügung stehende Internet-Anbindung bereits eine solche Lösung ;-) .

Allerdings gibt es eine Reihe von Unternehmen, die jede neue Technologie fast schon blind unterstützen. Deshalb wollen Sie unbedingt in ‘die Cloud’ - und sei es nur, damit sie auch ‘mithalten können’. Und natürlich sollen auch diese Daten gesichert werden.

Was aber bedeutet das **Backup aus der Cloud**, also die Sicherung Ihrer Cloud-Daten in der Praxis? - Hierzu möchte ich Ihnen die Übersetzung eines Artikels nicht vorenthalten, den einer der NetWorker Experten - Preston de Guise, mittlerweile bei Dell/EMC Australien tätig - im Juli 2019 in seinem Blog veröffentlicht hat. Ich habe den Artikel nicht vollständig übersetzt - zur besseren Verständlichkeit habe ich einige Details bewußt ausgelassen. Wollen Sie den Artikel im Original lesen, finden Sie den Link am Ende des Dokuments.

Die intelligenteste Methode zum Verschieben der Workload in eine öffentliche Cloud besteht darin, sie für die Ausführung als SaaS-basierte Anwendung vollständig überarbeitet zu haben. Ab diesem Zeitpunkt zahlen Sie für die Anwendung und ihre Datendienste. Nicht mehr - aber auch nicht weniger.

Ja, natürlich können Sie Ihre virtuelle Infrastruktur verschieben (sog. *lift & shift*). Es ist in der Regel kein Problem, eine vorhandene Anwendung von einem virtuellen Rechner (den Sie ja bereits erworben haben) in das Internet zu verschieben (Internet as a Service, IaaS). Allerdings ist dies garantiert auch die schnellste und effektivste Methode, Ihr jährliches IT-Budget bereits innerhalb eines Quartals aufzubrauchen. Das ist so bereits geschehen - und es passiert immer wieder.

Natürlich gibt es eine Vielzahl verschiedener Cloud-Betriebsmodelle. Hierbei ist Software-as-a-Service (SaaS) das Optimum an Einfachheit, das A und O in der Cloud-Welt. Und damit sind Ihnen Kopfschmerzen in gigantischen Ausmaßen sicher.

Laut dem Analystenhaus IDC.Data Protection besteht der australische Cloud-Markt vor allem aus SaaS Lösungen.

Die neuesten Zahlen von IDC für den Zeitraum 2016 bis 2018 ergaben, daß für Australien die Umsatzzahlen für den Cloud-Service enorm gestiegen sind, auf ca. 4,01 Milliarden US-Dollar im Jahr 2018. Mit jährlichen Wachstumsraten von 30,6.

"Die australische Cloud besteht zu 66 Prozent aus SaaS: IDC"
(Simon Sharwood, am 4. Juli 2019, Computer Reseller News, CRN Australia)

Simon beschreibt weiter, dass SaaS 65,8% dieser Ausgaben ausmachte - aufgerundet auf 66% für die Überschrift.

Eine Liste der größten SaaS-Unternehmen ist wie ein Who-is-Who von Technologie-Lieblingen, darunter Salesforce, Workday, ServiceNow, Tableau (mittlerweile von Salesforce gekauft), Zendesk und Mulesoft. Und natürlich sind heute die Office 365-Dienste Heute ein häufiger Ausgangspunkt für Unternehmen, die die Back-End-Verwaltung von E-Mails an eine andere Institution abgeben möchten.

Das Wichtigste dabei aber ist:

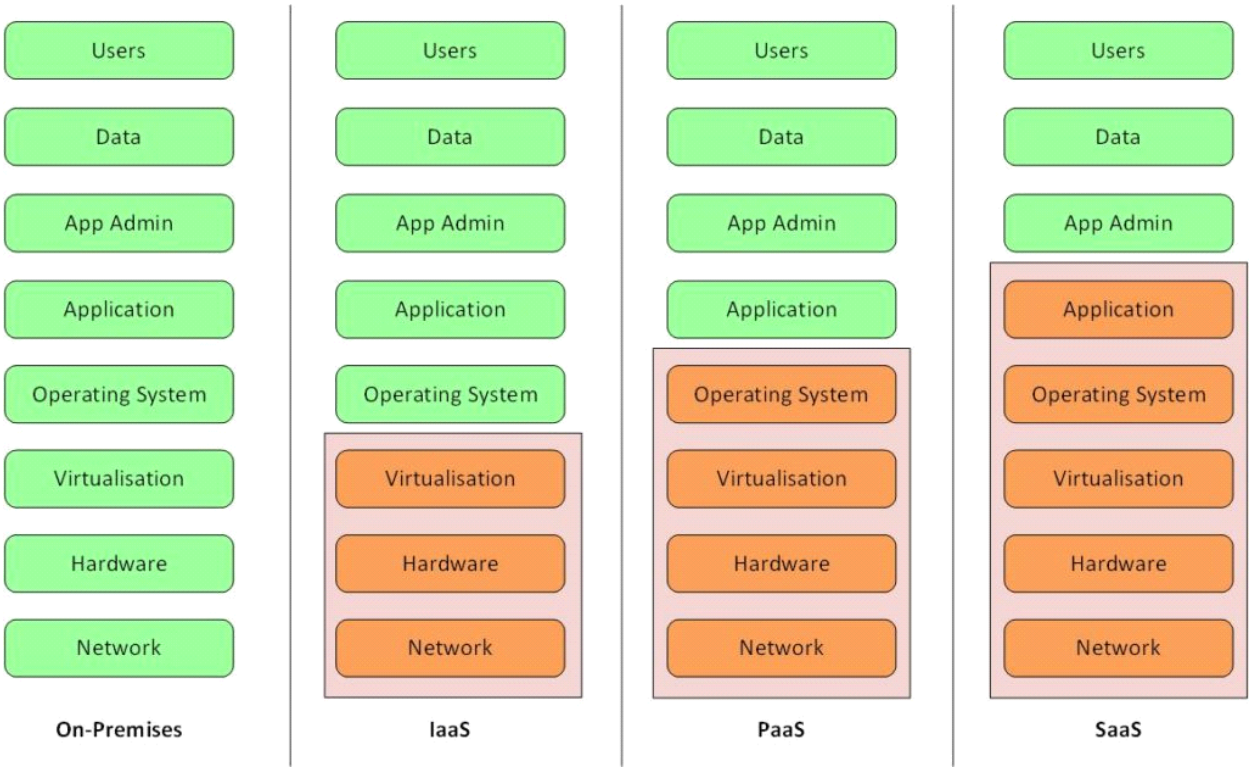
> **Jede SaaS-Anwendung, die Sie bereitstellen, erhöht die Komplexität, die Sie beim Nachverfolgen und Verwalten Ihres Datenschutzes haben. Das ist Fakt.**

Wann immer etwas vor Ort ausgeführt wird, gibt es immer irgendeine Möglichkeit, Ihre Daten zu schützen. Irgendwie wird es schon gehen. Evtl. akzeptieren Sie zunächst für das schnelle Wiederherstellungsziel (Recovery Time Objective, RTO) und den möglichst geringen Datenverlust (Recovery Point Objective, RPO) sowie zur Vermeidung von Systemabstürzen das Anlegen von Snapshots und/oder Sie führen Daten-Replikationen durch.

Selbst wenn es sich um eine Datenbank handeln sollte, finden Sie immer irgendeine Möglichkeit, diese zu sichern:

- Handelt es sich um einen traditionellen Datenbank-Hersteller, gibt es wahrscheinlich ein Datenbankmodul oder ein Plugin dafür.
- Wenn nicht, gibt es sicherlich andere Wege, Ihre Daten zu sichern: z.B. durch Pre-/Post-Verarbeitung, Daten-Dumps usw.

SaaS ändert dieses bekannte Bild. Ihre klassischen Servicemodelle sehen jetzt so aus:



On-Premesis	Innerhalb der Firma/der Niederlassung
IaaS	Infrastructure-as-a-Service
PaaS	Platform-as-a-Service
SaaS	Storage-as-a-Service

Dies Bild zeigt die herkömmliche, vollständige Datenverarbeitung beim Kunden (On-Premises) im Vergleich zu den In-Cloud-Zugriffsebenen - die rot eingefärbten Blöcke befinden sich außerhalb Ihrer Kontrolle.

Ich vergleiche SaaS mit NAS. NAS ist in IT-Infrastrukturkreisen praktisch allgegenwärtig, was zum einen die Präsentation von Datenspeichern und Diensten für Unternehmen vereinfacht, was allerdings auch mit Datenschutzproblemen verbunden ist. Tatsächlich verhält sich SaaS sehr ähnlich NAS. Im bereits erwähnten CRN-Artikel zitiert Simon Sharwood IDC mit den Worten:

> *„Unternehmen sind sich auch bewusst, daß bereitgestellte SaaS-Lösungen schwierig werden können. Um Informationssilos in der Cloud und lokal zu vermeiden, erforderrn SaaS-Anwendungen häufig die komplexe Integrationen mit lokaler Software. Dies bedeutet, daß das Unternehmen nicht schnell oder kostengünstig wechseln kann, selbst wenn eine innovativere SaaS-Anwendung verfügbar wird.“*
>
> *"Die australische Cloud besteht zu 66 Prozent aus SaaS: IDC",*
> (Simon Sharwood, am 4. Juli 2019, Computer Reseller News, CRN Australia)

Kurz gesagt: SaaS macht die Dinge wirklich einfach. Allerdings besteht eine relativ hohe Wahrscheinlichkeit, dass Sie zur Geisel Ihrer Daten werden, nachdem Sie die Last von Ihren eigenen Lösungen in die SaaS-Umgebung verschoben haben. Schuld daran ist vor allem die Vielzahl der SaaS-Anwendungen: Es gibt Tausende und Abertausende - und wahrscheinlich sogar noch mehr.

Die alte Herausforderung in der lokalen IT besteht darin, dass ein neues System oder eine neue Aufgabe vollständig bereitgestellt und in die Produktion übernommen werden kann, bevor jemand sagt: "Und wie lösen wir die Backups?"

In gewissem Maße gelang es Frameworks wie ITIL (*IT Infrastructure Library*), die Kontrolle über das System sicherzustellen. Dies wird durch das Einfügen von Grenzen sowie durch andere Steuerungsmechanismen erreicht. Dies setzt allerdings voraus, dass die Anbieter von Systemen und Anwendungen nachweisen, dass sie alle erforderlichen Voraussetzungen für die Migration von einem Build- bzw. Entwicklungsstatus zu einem Produktionsstatus erfüllen.

Natürlich waren ITIL-artige Kontrollen genau das, was das Unternehmen benötigte, um chaotische Datenrisiken in seinen Umgebungen zu vermeiden; und sie trugen zweifellos dazu bei, daß Unternehmen nach öffentlichen Cloud-Diensten suchten, weil es „*... die IT zu schwierig macht, Dinge zum Laufen zu bringen*“.

So, das ist es also (mit einem Augenzwinkern auf Firefly ???):

- SaaS ist cool
- SaaS ist beliebt
- SaaS ist das ultimative Ziel für die Arbeiten, die in der Public Cloud ausgeführt werden,
  und…
- **SaaS verfügt über <u>keinen</u> gemeinsamen Mechanismus, mit dem ein Unternehmen seine Daten schützen, sichern, wiederherstellen oder extrahieren kann.**
- **Für SaaS gibt es kein NDMP!**

Es ist verrückt. Und es ist nichts, was Sie Anbietern von Datensicherungslösungen so direkt vermitteln können: "Dies ist Euer Problem. Behebt es!" - Hier ist die leider unangenehme Wahrheit: "Es bleibt Dein Problem!"

Es tut mir leid, dass ich darüber 'predige', aber genau das ist der Haken. Jedes Mal, wenn Sie eine andere SaaS-Anwendung in Ihrem Unternehmen einsetzen, ohne genau zu wissen, wie Sie die Umgebung, in der Sie tätig sind, schützen, entsteht ein Risiko. Und dieses Risiko liegt bei Ihnen und auch nicht bei Ihren lokalen Datenschutzanbietern, ganz egal, um wen es sich handelt.

Das soll nicht heißen, dass die Anbieter von Sicherungslösungen sich nicht darum kümmern. Jemandem, der solche Lösungen anbietet, liegt daran, dass er mit Leidenschaft dafür sorgt, daß die Daten seines Kunden auch geschützt werden.

Vertrauen Sie mir, denn es ist die Wahrheit:

> Ich arbeite seit über 20 Jahren mit IT-Gruppen, Unternehmen und Führungskräften auf allen Ebenen zusammen, um allen zu helfen, die Notwendigkeit umfassender Datenschutzdienste zu erkennen und unzusetzen. Und trotzdem muss ich sie noch regelmäßig überprüfen und den alten Einwand " ... aber wir müssen doch nicht ..." korrigieren, der bereits vor mehr als 20 Jahren hätte begraben werden sollen. Sie können jedoch nicht in dieser Branche tätig sein, wenn Sie sich nicht auch darum kümmern wollen.

Bereits vor zwei Jahrzehnten wurde erkannt, daß es zur Datensicherung im NAS gewisser standardisierter Mechanismen bedurfte. Und obwohl NDMP natürlich auch seine Grenzen hatte, gab es doch einen einheitlichen Mechanismus, der es erlaubte, NAS-Daten zu sichern und wiederherzustellen.

Seien wir ehrlich: Fast jeder kann mit seinem Laptop, einem grundlegenden Verständnis der Codierung und einer Kreditkarte ein SaaS-Geschäft eröffnen, wenn er einen Schlüsselkunden gewinnen möchte. Wahrscheinlich gibt es genau deshalb eine so unüberschaubar große Anzahl von SaaS Entwicklern. Allerdings ist ein Konsens darüber, dass "*... SaaS Anbieter APIs für die Sicherung und Wiederherstellung bereitstellen*" wahrscheinlich fast so schwierig, wie Donald Trump dazu zu bringen, etwas zu sagen, das sowohl schlüssig und zugleich wahr ist.

Es bleibt uns keine Wahl - wir müssen mit diesem Problem leben.

Die Lösung wird nicht über Nacht kommen und auch nicht von den Anbietern der Datensicherungs-Lösungen. Diese klappern bereits jeden einzelnen SaaS-Anbieter auf dem Markt ab und sprechen mit ihnen. Doch es gibt einfach zu viele.

Eine Lösung wird es nur durch die Zusammenarbeit von Ihnen und den SaaS Anbietern geben.

- Das Unternehmen, das ein SaaS-Produkt anbietet, ist dafür verantwortlich, einen dokumentierten Mechanismus für die vom Abonnenten initiierte Sicherung und Wiederherstellung bereitzustellen.

- Als Kunde einer SaaS-Lösung sind Sie dafür verantwortlich, sicherzustellen, dass die von Ihnen abonnierte SaaS-Lösung über diese Funktionalität verfügt. Fordern Sie diese an, wenn sie nicht vorhanden sein sollte.

Erst wenn es eine garantierte Sicherungs- und Wiederherstellungsmethode gibt, kann auch eine Gesamtlösung erstellt werden. Für diese Lösung müssen Sie sich jedoch mit Sicherheit richtig anstrengen und in Ihren Teams (Vertrieb, IT und Management) das Bewußtsein über die Risiken und Gefahren schärfen, die Sie sich durch eine SaaS Lösung ins Haus holen, für die es noch keine Backup/Recovery Lösung gibt.

> Sinngemäß übersetzt (aus dem Australischen ;-) von Carsten Reinfeld nach Preston de Guise (Advisory Systems Engineer bei EMC) Artikel von dieser URL:

https://nsrd.info/blog/2019/07/06/the-perfect-cloud-environment-is-the-perfect-headache-for-data-protection/