

# Cloud vs. (eigene physische) Server – Chancen und Risiken

*„Soll ich's wirklich machen oder lass ich's lieber sein?“*

Prof. Dr. Christian Baun

Frankfurt University of Applied Sciences  
(1971–2014: Fachhochschule Frankfurt am Main)  
Faculty of Computer Science and Engineering  
[christianbaun@fb2.fra-uas.de](mailto:christianbaun@fb2.fra-uas.de)

# Agenda

- Klassische/traditionelle IT
- Grundlagen des Cloud Computing

*„There is no cloud – it’s just someone else’s computer“ (Quelle: Unbekannt)*

- Unterschiede Cloud vs. (eigene physische) Server
  - Chancen
  - Risiken

# Klassische/Traditionelle IT

- Betrieb physische Server-Hardware vor Ort („*On-Premises*“) u.a. für:
  - Datenhaltung (Speicher)
  - Archivierungssoftware
  - Betrieb von Branchensoftware
  - Betrieb von (Server-)Anwendungen (z.B. Mailserver/Webserver/etc.)
  - Buchhaltung
  - Kundenbeziehungsmanagement (CRM)



# Cloud Computing – Dienste/Services

- Cloud Computing ist ein Sammelbegriff für verschiedene **Dienste**
  - Ein Dienstanbieter (*Service Provider*) stellt eine IT-Dienstleistung für einen oder mehrere Kunden (*Customer*) bereit
    - Dienstanbieter = externer Anbieter oder unternehmenseigene Abteilung
  - Übliches Szenario: **Outsourcing**  $\implies$  Auslagern von IT-Dienstleistungen
  - Funktionsumfang und Dienstgüte sollten über ein **Service-Level-Agreement (SLA)** definiert sein

Wie unterscheidet man Cloud-Dienste **organisatorisch**?

# Organisatorische Unterscheidung der Dienste

- **Öffentliche Dienste** (Public Cloud)
  - Anbieter und Kunden gehören unterschiedlichen Organisationen an  
⇒ **Outsourcing**
  - (Fast) keine Kosten für Anschaffung, Betrieb und Wartung eigener Hardware
  - Ressourcen sind sofort einsatzbereit und (fast) unbegrenzt verfügbar
- **Private Dienste** (Private Cloud)
  - Anbieter und Benutzer gehören der gleichen Organisation an
  - Kosten ähnlich einer nicht-Cloud-basierten Architektur
  - Basiert auf klassischer/traditioneller IT
- **Hybride Dienste** (Hybrid Cloud)
  - Öffentlich verfügbare und private Dienste werden gemeinsam verwendet
  - Einsatzbeispiele:
    - Lastspitzen mit öffentlichen Diensten abfedern
    - Sicherheitskopien in öffentliche Dienste auslagern

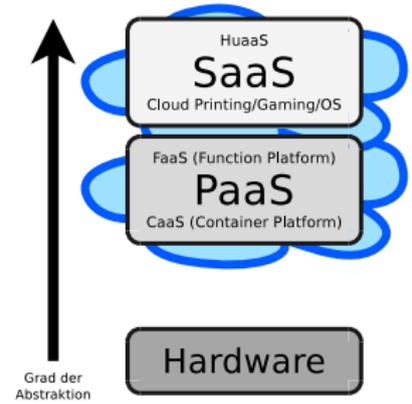
Welche **funktionalen** Gruppen von Cloud-Diensten gibt es?



# Funktionale Unterscheidung der Dienste – PaaS + FaaS

## ● Plattformdienste (PaaS)

- Anbieter betreibt skalierbare Laufzeitumgebung(en)
- Kunden betreiben eigene Webanwendungen in der Infrastruktur des Dienstansbieters
  - Anwendungen können verschiedene Infrastruktur- und Speicherdienste nutzen
- Zielgruppe: **Entwickler und Betreiber von Webanwendungen**



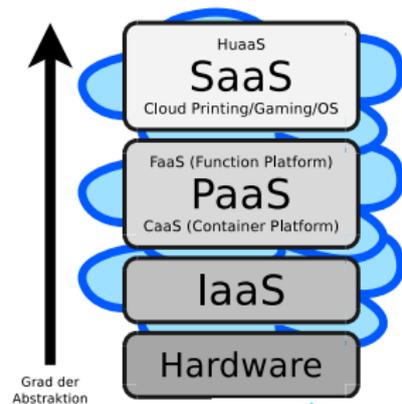
Function as a Service (FaaS) sind eine Untergruppe der PaaS

- Kunden können ihre eigenen Funktionen (skalierbar) in der Infrastruktur des Dienstansbieters ausführen
- Typischerweise unterstützen die Dienste JavaScript (Node.js), Python und/oder Java
- Funktionen werden durch externe Anforderungen oder Ereignisse ausgelöst (z.B. HTTP-Anfrage, Empfang einer E-Mail,...)
- Das Backend ist für die Kunden *unsichtbar* ⇒ **Serverless Architecture/Computing**

# Funktionale Unterscheidung der Dienste – IaaS

## ● **Infrastrukturdienste (IaaS)**

- Anbieter betreibt physische Server
- Kunden betreiben **virtuelle Maschinen (VM)** mit (fast) beliebigen Betriebssystemen und unveränderten Anwendungen
  - Kunden haben in ihren VMs Administratorenrechte und definieren die Firewall-Regeln



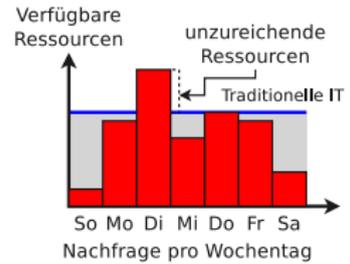
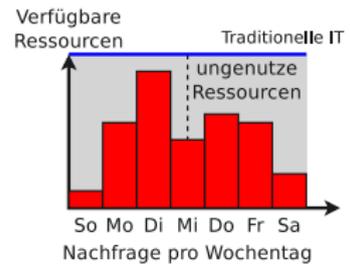
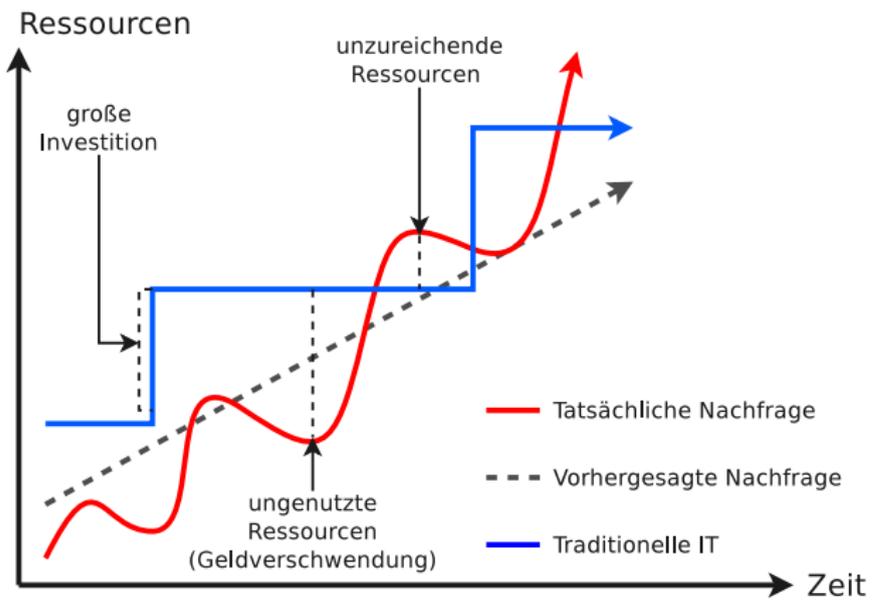
In einem IaaS-Angebot kann ein komplettes Rechenzentrum virtuell abgebildet werden

- IaaS-Angebote großer Dienstleister beinhalten in der Regel verschiedene Dienste für VMs, Speicher (Objektspeicher und Blockspeicher), Datenbanken, virtuelle Netze, IP-Adressen, Firewalls, Lastverteiler, etc.





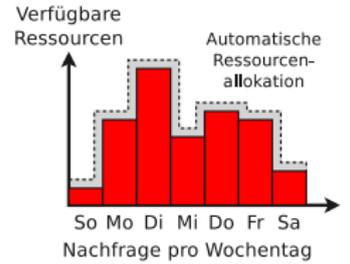
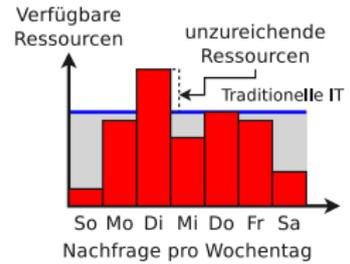
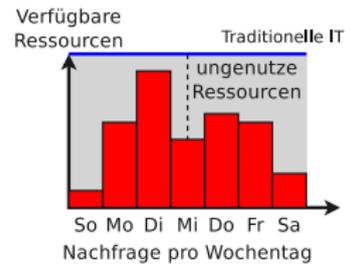
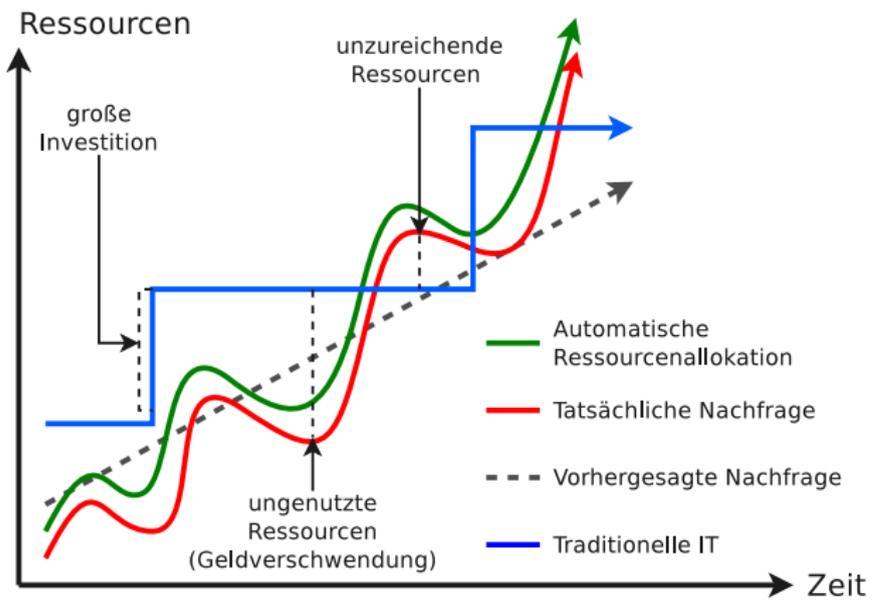
# Chancen: IaaS vs. eigene physische Infrastruktur (2/3)



## Problem 2: Vorhergesagte Nachfrage ≠ tatsächliche Nachfrage

- Ungenutzte Ressourcen beim traditionellen IT-Modell
- Eventuell unzureichende Ressourcen, wenn die Nachfrage unerwartet schnell steigt

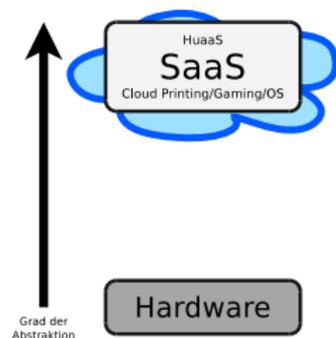
# Chancen: IaaS vs. eigene physische Infrastruktur (3/3)



- Ziel: Virtuelle Infrastruktur**
- Keine hohen Investitionskosten
  - Immer ausreichend viele Ressourcen verfügbar
  - Automatische Anpassung je nach Nachfrage

# Chancen: SaaS vs. lokal installierte Anwendungen

- Vorteile für Kunden
  - Zur Nutzung ist nur ein Browser nötig
  - Betriebssystemunabhängigkeit
  - Kein Installationsaufwand
  - Kein Wartungsaufwand (Updates)
  - Ortsunabhängig nutzbar



Große Dienstleister haben durch Mitarbeiterstärke und Erfahrung eine gewaltige Kompetenz.

- Vorteile für Dienstleister:
  - Keine Raubkopien
  - Alle Kunden haben automatisch die aktuellste Softwareversion
  - Geringerer Supportaufwand

## Chancen: Geringere Kosten

- Cloud-Dienste verursachen (fast) keine Anschaffungskosten und (eventuell) geringere Betriebskosten als eigene physische Ressourcen

Dass Cloud-Computing immer die preisgünstigste Alternative ist, kann man nicht pauschal sagen!

- Die Nutzung einer **SaaS** anstatt einer gekauften Software verursacht **in der Regel** deutlich geringere Anschaffungskosten
  - Weitere Aussagen zu SaaS sind nicht pauschal möglich
- Die Nutzung einer **IaaS** anstatt eigener physischer Server vor Ort verursacht **immer deutlich geringere** Anschaffungskosten
  - Bei flexibler Nutzung („Pay-as-you-go-Prinzip“) sind die Betriebskosten meist sehr hoch (evtl. ist IaaS dann sogar die teuerste Alternative!)
  - Bei Mietverträgen über 1 oder 3 Jahre sinken die Kosten deutlich, aber die Kunden binden sich  $\implies$  kein richtiges „Pay-as-you-go-Prinzip“ mehr!

Wer seinen Ressourcenbedarf kennt, kann die Kosten zur Nutzung einer IaaS exakt berechnen

Amazon AWS Simple Monthly Calculator: <https://calculator.s3.amazonaws.com/index.html>

Microsoft Azure Preisrechner: <https://azure.microsoft.com/de-de/pricing/calculator/>

# Wie steht es mit den Risiken?

Bildquelle: Pixabay (CC0)

- Fragen die sich jeder stellen muss, bevor er sich gegen eigene physische Hardware vor Ort und für Outsourcing entscheidet:
  - 1 Wie ist die **Verfügbarkeit** der Daten und Dienste?
    - Was ist die Konsequenz, wenn die garantierte Verfügbarkeit unterschritten wird?
    - Was, wenn der Dienstanbieter den Dienst verändert oder einstellt?
  - 2 Kann es zum **Datenverlust** kommen?
    - Was ist die Konsequenz von Datenverlust?
  - 3 Sind eigene Daten **sicher vor fremdem Zugriff**?
    - Was ist die Konsequenz eines Diebstahls?
  - 4 Sind die Dienstanbieter **vertrauenswürdig**?
    - Wer hat Zugriff auf die Daten der Kunden?
  - 5 Können Kunden einen **Dienstanbieter verlassen**?
    - Gibt es vergleichbare Angebote/Lösungen?



# (1) Verfügbarkeit von Cloud-Diensten

Es war die schlimmste Erfahrung seines Berufslebens. „**Zwei Tage lang war unsere Firma komplett lahmgelegt**“ ... „Sie können sich gar nicht vorstellen, was hier los war!“ ... Niemand in der ganzen Firma konnte mehr auf irgendein internes Dokument zugreifen; Kunden wunderten sich, dass ihre E-Mails unbeantwortet blieben; **48 Stunden lang war die Firma ohne Daten und Büro-Software**. Dabei war ... technisch alles in Ordnung, die Computer liefen, die Datenleitungen funktionierten. Der Grund für den Totalausfall ... ein **Fehler im Bezahlssystem von Google**.

Weil ein Rechnungsbetrag von wenigen Hundert Euro nicht abgebucht werden konnte, hatte der kalifornische Gigant der deutschen Firma kurzerhand den Zugang zu ihrer Büro-Software und den zugehörigen Unterlagen gesperrt. Ohne Vorwarnung. „Am liebsten hätte ich das Geld in einen Umschlag gepackt und persönlich hingetragen“ ... Aber er habe nicht einmal gewusst, wohin. Für mittelständische europäische Kunden ist die Google-Niederlassung in Dublin zuständig, **telefonisch erreichbar ist sie jedoch nicht**. Und jene Hilferufe, die der ... per E-Mail schickte und ins Formular auf der Google-Website eintrug, blieben zunächst unerhört.

Quelle: Dirk Asendorpf, Die Zeit, 17. Februar 2011, S.39  
<https://www.zeit.de/2011/08/Cloud-Computing>

- Dass lokal installierte Software nicht funktioniert bzw. erreichbar ist, kann immer passieren
- Bei Cloud-Diensten sind Kunden aber komplett von der Erreichbarkeit und Hilfsbereitschaft des Anbieters abhängig

Was kann man erwarten, wenn etwas schief läuft?

# (1) Verfügbarkeit von Cloud-Diensten (Beispiel: AWS S3)

- Amazon garantiert 99.9% monatliche Verfügbarkeit für S3

Verfügbarkeit	Downtime (HH:MM:SS)		
	pro Tag	pro Monat	pro Jahr
99.9%	00:01:26	00:43:49	08:45:56
99%	00:14:23	07:18:17	87:39:29

- Wird die Verfügbarkeit unterschritten, erhält man eine **Gutschrift**
  - <http://aws.amazon.com/s3-sla/>

Prozentsatz monatlicher Systemverfügbarkeit	Prozentsatz Servicegutschrift
Gleich oder größer als 99,0% aber geringer als 99,9 %	10 %
Geringer als 99,0 %	25 %

Bei IBM und Microsoft sind die Zahlen fast gleich

- [https://azure.microsoft.com/de-de/support/legal/sla/storage/v1\\_5/](https://azure.microsoft.com/de-de/support/legal/sla/storage/v1_5/)
- <https://www-03.ibm.com/software/sla/sladb.nsf/sla/bm-7857-04>

Was hilft eine Gutschrift weiter, wenn der Dienst und damit die eigenen Daten unerreichbar sind?

# (1) Bricht die Cloud zusammen, bricht das Haus zusammen

downdetector.com <sup>!</sup>



Google Cloud is a suite of cloud computing services for developers, offering infrastructure as a service, Platform as a service and Serverless Computing features. Google Cloud



Bildquelle: Public Domain

June 2nd 2018

<http://www.zdnet.com/article/google-cloud-goes-down-taking-youtube-gmail-snapchat-and-others-with-it/>

A mysterious outage has hit Google Cloud... and thousands of sites have gone down as a result, including both Google and non-Google services.

Affected companies include ... Snapchat, Vimeo, ... YouTube, Gmail, Google Search, G Suite, Hangouts, Google Drive, Google Docs, Google Nest...

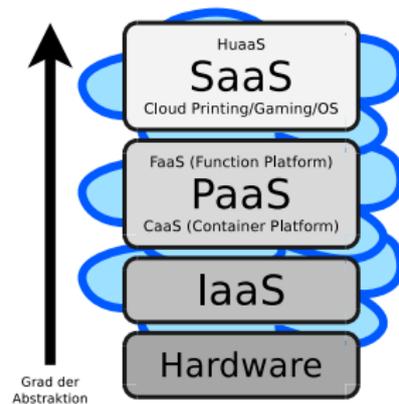
<http://www.fastcompany.com/90358396/that-major-google-outage-meant-some-nest-users-couldnt-unlock-doors-or-use-the-ac>

... But an especially annoying side effect of Google Cloud's downtime was that Nest-branded smart home products for some users just failed to work. According to reports from Twitter, many people were unable to use their Nest thermostats, Nest smart locks, and Nest cameras during the downtime. This essentially meant that because of a cloud storage outage, people were prevented from getting inside their homes, using their AC, and monitoring their babies...

Schöne neue Welt? Funktionieren Ihre Geräte auch ohne Verbindung zum Cloud-Dienstleister bzw. ohne Internetverbindung?

# (1) Dass Dienstangebote sich ändern, ist quasi Alltag

- In **SaaS**-Dienstangeboten ändern sich häufig Funktionsumfang und GUI
  - Bei lokal installierter Software hat es der Kunde selbst in der Hand wann er „wechselt“
- In **PaaS**- und **IaaS**-Dienstangeboten ändern sich häufig Funktionsumfang und Werkzeuge
  - Man muss kontinuierlich „am Ball bleiben“
  - Änderungen durch den Dienstanbieter ziehen meist Anpassungsaufwand nach sich
- Unterschied zwischen **Parental Computing** und **Personal Computing**



## Sehr lesenswerte Quelle

### The Cloud's My-Mom-Cleaned-My-Room Problem

Welcome to the era of parental computing, or how the cloud makes children of us all

<https://www.theatlantic.com/technology/archive/2011/09/the-clouds-my-mom-cleaned-my-room-problem/245648/>

Die hier beschriebenen Änderungen durch die Dienstanbieter sind bei weitem nicht das schlimmste Szenario (siehe nächste Folie).

# (1) Und wenn der Dienstanbieter den Dienst ganz einstellt?

- Temporäre Dienstaussfälle sind immer möglich
  - Es kann auch jederzeit vorkommen, dass ein Anbieter ein Dienstangebot verändert oder ganz einstellt



- Public Cloud IaaS-Dienstangebot von Hewlett-Packard (HP)
- 30.10.2015: Ankündigung, dass der Dienst am 31.1.2016 abgeschaltet wird

- 09/2016: Microsoft bietet gemeinsam mit T-Systems als Datentreuhänder ein IaaS-Dienstangebot für datenschutzbewusste Kunden



Warum ein unabhängiger Datentreuhänder hier relevant ist, zeigt Folie 25.

- 08/2018: Microsoft kündigt das Angebot ab und akzeptiert keine Neukunden
- 08/2019: Microsoft integriert zwei neue Rechenzentren in Deutschland mit „sehr hohem Datenschutzniveau“ in sein IaaS-Dienstangebot – allerdings ohne unabhängigen Datentreuhänder

- Public Cloud Speicherdienst von Nirvanix
- 16.9.2013: Ankündigung, dass der Dienst am 30.9.2013 abgeschaltet wird

Wie lange dauert eigentlich der Export von Daten aus einem Cloud-Dienst (siehe nächste Folie)?

- Das Unternehmen erklärte sich am 1.10.2013 für insolvent



# (1) Übertragungsdauer großer Datenmengen bedenken

- Eine Festplatte mit 10 TB Speicherkapazität kostet aktuell ca. 300 €
  - 10 TB sind heute (2019) also eine recht überschaubare Datenmenge
- Szenario:
  - Ein Kunde speichert 10 TB Daten in einem Cloud-Speicherdienst, mit dem er nicht mehr zufrieden ist, oder der in Kürze seinen Betrieb einstellt
- Aufgabe: Berechnen Sie die Übertragungsdauer für 10 TB für folgende Datentransferraten: 10 MBit/s, 100 MBit/s und 1000 MBit/s

$$10 \text{ TB} = 10 * 2^{40} \text{ Byte} = 10.995.116.277.760 \text{ Byte} = 87.960.930.222.080 \text{ Bit}$$

- Für 10 MBit/s Datentransferrate:

$$\frac{87.960.930.222.080 \text{ Bit}}{10.000.000 \text{ Bit/s}} \approx 8.796.093 \text{ s} \approx 2443,3 \text{ h} = \text{mehr als 100 Tage}$$

- Für 100 MBit/s Datentransferrate: ca. 10 Tage
- Für 1000 MBit/s Datentransferrate: ca. 1 Tag

Die Übertragung großer Datenmengen war noch nie trivial.  
Beim Einsatz von Cloud-Diensten ist ein „Plan B“ immer sinnvoll.

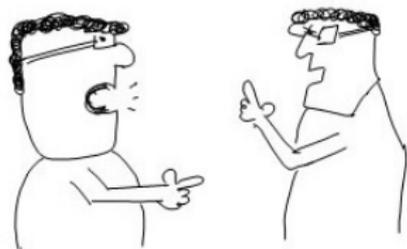
## (2) Möglichen Datenverlust bedenken und vorbeugen

- Datenverlust bei der Nutzung **eigener physischer Hardware vor Ort** ist immer möglich

- Gründe: Benutzerfehler, technische Fehler, Schadsoftware (Viren und Trojaner), Elementarschäden, Diebstahl (Vandalismus)...

WHERE THE HECK  
IS MY DATA?

ITS THERE, UP  
IN THE CLOUDS.



Brainstuck.com

- **Exakt die gleichen Gefahren gibt es bei Cloud-Dienstanbietern**
  - Diese Unternehmen haben zwar viel Personal und Erfahrung, 100% Sicherheit ist aber unmöglich
  - Es gibt zahlreiche Beispiele für Datenverlust in Cloud-Diensten

Datenverlust in Cloud-Diensten ist nicht nur ein theoretisches Szenario!

## (2) Datenverlust ... nicht nur ein theoretisches Szenario



Microsoft Azure

- **Microsoft 365 und Azure SQL (Januar 2019)**
- Einige Dienste für einen Tag nicht erreichbar (gestört)
- Einige Kundendaten (SQL-Datenbanken) dauerhaft verloren



- **Salesforce (Mai 2016)**
- Ein Serverstandort der SaaS für einen Tag nicht erreichbar
- Einige Kundendaten dauerhaft verloren



- **Amazon AWS (April 2011)**
- Tausende Webseiten für Tage offline
- Einige Kundendaten dauerhaft verloren
- Betroffene Kunden bekamen **zehn Tage kostenlose Nutzung** (siehe Folie 17)



- **Google Gmail (Februar 2011)**
- Mails/Kalender/Kontakte von 150.000 Kunden (teils dauerhaft!) gelöscht

Migration in einen Cloud-Dienst ersetzt kein lokales Backup!

## (3) Sicherheit eigener Daten vor fremdem Zugriff

- Betreibt ein Kunde virtuelle Server in einem IaaS, muss er selbst für deren Sicherheit sorgen – genau wie bei physischen Servern vor Ort
  - Einzig der Schutz des Gebäudes ist nicht mehr in der eigenen Hand
- Passwörter sind nicht mehr/weniger sicher, wenn ein Server bei einem Cloud-Dienstanbieter läuft
  - Betriebssysteme und Netzwerkdienste regelmäßig aktualisieren!
    - Bei neuen Sicherheitslücken auch sehr kurzfristig

Auch bei SaaS kann es Sicherheitsprobleme geben

Dropbox wurde an dieser Stelle als Beispiel gewählt, weil dieser Anbieter Sicherheitslücken sehr transparent kommuniziert.



- 2011: Dropbox akzeptierte 4 Stunden lang beliebige Passwörter für alle Benutzerkonten
- 2012: 68 Millionen Kundenzugangsdaten wurden gestohlen
- 2016: Die Zugangsdaten aus dem Jahr 2012 wurden im Darknet zum Verkauf angeboten und waren schon in den vier Jahren zuvor im Umlauf

Eine 100%tige Sicherheit gegen den Diebstahl eigener Daten gibt es nicht.  
Zwei-Faktor-Authentisierung und konsequente Verschlüsselung hilft aber!

## (4) Datenzugriff durch Behörden im Ausland

- Amerikanische Unternehmen unterliegen u.a. dem **Patriot Act** (2001) und **CLOUD Act** (2018)
  - Die Unternehmen müssen US-Behörden auch dann Zugriff auf Daten gewährleisten, wenn die Speicherung nicht in den USA erfolgt
  - Den Unternehmen kann von der anfragenden Behörde untersagt werden, ihre Kunden über eine Datenabfrage zu informieren

Microsoft hat schon im Juni 2011 klargestellt, das US-Unternehmen alle Kundendaten an US-Behörden auf deren Anfrage hin herausgeben müssen. Kunden würden informiert wo immer das möglich ist, aber kein US-Unternehmen kann garantieren, das eine Information der Kunden von der anfragenden Behörde erlaubt wird.

<http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225>



Alibaba Cloud

- Es gibt auch große Cloud-Diensteanbieter, die keine US-Unternehmen sind
- Ein bekanntes Beispiel ist die Alibaba Cloud aus China
- China ist ein „Sozialistisches Einparteiensystem“  
⇒ keine unabhängige Justiz, intransparente Behörden, Überwachung...

- Lösung: Dienstangebote aus Deutschland/Europa nutzen
- Unsere Anbieter sind aber relativ klein (wir haben keine Technologietreiber!)

## (5) Risiko des Lock-in

- Entscheidet sich ein Kunde für einen öffentlichen Dienst, entscheidet er sich auch für eine Schnittstelle
- Gefahr: **Lock-in**
  - Abhängigkeit zwischen Dienstanutzer und -anbieter
- Szenarien: Preiserhöhung, Insolvenz des Anbieters, Änderung des Dienstangebots (Funktionalität),...
- Wechsel des Anbieters nur bei gleichzeitigem **Verlust** der Infrastruktur (**Dienste**) und eventuell sogar der **Daten**
  - Auswirkungen für Kunden (insbesondere Unternehmen) u.U. fatal
- Verwendet man einen Dienst langfristig, **investiert** man in diesen
  - Das eigene Geschäftsmodell wird darauf ausgerichtet
  - Mitarbeiter werden geschult
  - Dienste werden *veredelt*

Gut, wenn man immer einen „Plan B“ hat...

# (5) Vermeidung des Lock-in (am Beispiel des AWS S3)

- **Wettbewerber**

- Bieten öffentliche Dienste mit gleicher Funktionalität und API
  - Für S3: Google Cloud Storage, HP Cloud Object Storage (†2016) , Connectria CS, Host Europe CS (†2014), Nirvanix (†2013), Dunkel Cloud Storage, Clouddian, IBM Cloud Object Storage. . .



- **(Freie) Lösungen**

- Betrieb eigener privater Dienste mit gleicher Funktionalität und API
  - Für S3: Eucalyptus Walrus, Nimbus Cumulus, OpenStack Swift, Riak CS, Ceph Object Storage, Minio. . .



MINIO



openstack  
CLOUD SOFTWARE

riak



Es gibt häufig Wettbewerber und/oder freie Reimplementierungen. Der Markt ist allerdings nicht statisch und freie Softwareprojekte kommen und gehen. Die Einarbeitung in Konkurrenzangebote und freie Reimplementierungen ist selten trivial.

# Fazit

- Diese Präsentation zeigte **viele Risiken** des Cloud-Computing
  - Es ist aber eine **spannende Technologie mit sehr viel Potential** bzgl.
    - Automatisierung, Flexibilität, Anschaffungs- und Betriebskosten, etc.
- Einige Grundregeln:
  - ① Eigene Anforderungen klären  $\implies$  Marktanalyse
    - Passendes Dienstangebot finden und Lock-In vermeiden!
    - Existieren Konkurrenzangebote und/oder freie Implementierungen?
    - „Plan B“ haben und austesten, bevor es nötig ist
  - ② Herkunft des Diensteanbieters und rechtliche Rahmenbedingungen klären
    - Verlässlichkeit des Diensteanbieters abschätzen
    - Anbieter aus Deutschland sind besser „greifbar“
    - Große Anbieter bleiben tendenziell länger im Geschäft
  - ③ Immer noch ein zweites Backup haben
    - Entweder lokal gespeichert oder bei einem anderen Dienstleister abgelegt
  - ④ Verschlüsselung und gute Passwörter nutzen
    - Mehr Sicherheit als Passwörter bietet Zwei-Faktor-Authentisierung

Die Installation eines Servers in einem Unternehmen dauert mehrere Wochen. Die Bereitstellung eines virtuellen Servers in einer IaaS dauert weniger als 5 Minuten.