

# Ein Blick in die Cloud

## Workshop Cloud Computing und Informationssicherheit

04.11.2011

Hochschule Bremen

# Nutzungsformen der Cloud

Firma A



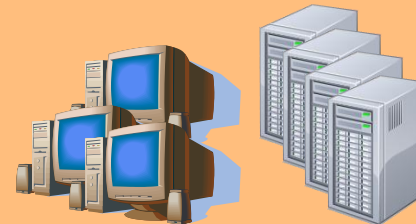
INTERNET



Software as a Service



Platform as a Service



Infrastructure as a Service

Firma B



# Vorteile der Cloud (Beispiele)

- Mehrere Kunden können die Systeme gleichzeitig nutzen, wodurch sich laufende Kosten für Räume und Verfügbarkeit auf mehrere Kunden verteilen.
- Die Virtualisierung ermöglicht kürzere Reaktionszeiten auf neue Systemanforderungen.
- Lastspitzen können kurzfristig durch zusätzliche Systeme abgedeckt werden.
- Eine Abrechnung nach Kriterien wie Dauer, Rechenleistung, etc. stellt den direkten Bezug zwischen IT-Leistung und Kosten her.
- Die Nutzer steuern die Systemauswahl, die Inanspruchnahme von IT-Ressourcen und deren Verfügbarkeit selbst und einzelfallbezogen.
- Spezialsysteme (CAD, Simulationen) können fallbezogen genutzt werden und sind somit zu niedrigeren Kosten verfügbar.

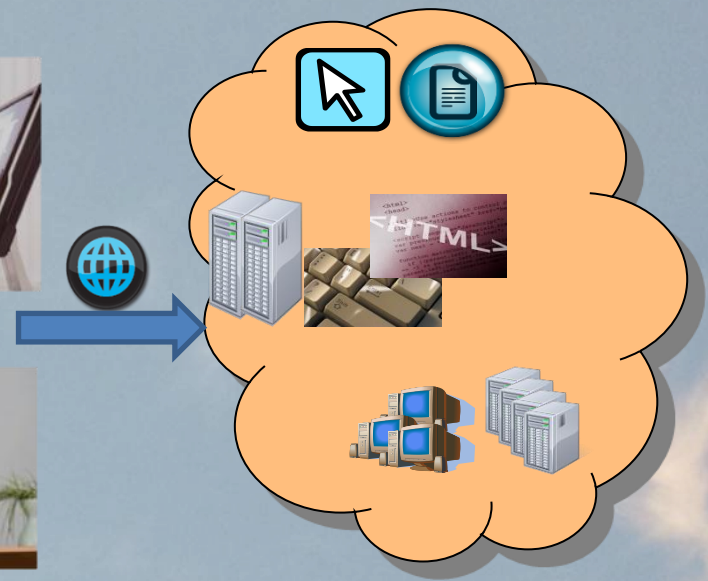
# Merkmale der Cloud

- Geteilte Ressourcen
- Massiv skalierbar
- Elastizität
- Nutzungsbezogene Abrechnung
- Selbstversorgung mit Ressourcen

Firma A



Firma B



Was bedeutet das?

# Geteilte Ressourcen

- Jeder Nutzer kann Informationen über das Hostsystem bekommen, in dem er seinen Teil des Hostsystems untersucht.
- Der Angreifer kann in unmittelbarer Nachbarschaft sitzen, z.B. auf demselben Host.
- Ein Angreifer muss nicht das virtuelle System angreifen, das Hostsystem kann ebenfalls zum Ziel führen (z.B. durch Speicheranalyse).

# Massiv skalierbar

- Der Anbieter bestimmt die Menge der maximal verfügbaren Ressourcen (Systeme, Bandbreite oder Speicher).
- Unabsichtliche oder absichtlich große Skalierungen können ein Hostsystem blockieren – oder die Skalierung muss verweigert werden.
- Erweiterung und Reduktion müssen durchgeführt und kontrolliert werden – wer übernimmt das?

# Elastizität

- Auch hier bestimmt der Anbieter die Grenzen und wägt Elastizität gegen Verfügbarkeit ab.
- Kurzfristig können Ressourcen durch Nutzer verringert oder erhöht werden. Nutzer beeinflussen so direkt die Leistungsfähigkeit der Systeme – positiv wie negativ.
- Wenn Nutzer allein über die Freigabe von Ressourcen bestimmen, können sie Ressourcen blockieren – oder sie bestimmen nicht allein.

# Nutzungsbezogene Abrechnung

- Die Erfassung der Details zur Nutzung erlaubt Rückschlüsse auf die Situation des Nutzers.
- Wer die Rechnung anzweifelt, hat es schwer Nachweise auf den virtuellen Ressourcen zu finden, insbesondere wenn diese bereits wieder freigegeben wurden.
- Fehlkonfigurationen und Angriffe können durch eine erhöhte Nutzung von Ressourcen direkt finanziellen Schaden anrichten.



# Selbstversorgung mit Ressourcen

- Die Menge und Art der bereits verwendeten Ressourcen kann sich augenblicklich ändern, trotzdem muss die Kompatibilität zur restlichen IT gewährleistet sein.
- Dem zuvor 2-stufigen Prozess (bestellen und genehmigen) fehlt nunmehr der Kontrollschritt.
- Der Zugriffspunkt auf die Ressourcen ist, mit Blick auf die Informationssicherheit, als kritisch einzustufen.

# Der sichere Weg in die Cloud

- Bisherige Erfahrungen, Leitfäden und Standards zum dienstleistungsbezogenen Outsourcing sind hilfreich.
- Etablierte Sicherheitsprozesse im Outsourcing, z.B. die Trennung von Bestellung und Freigabe, müssen übertragen werden.
- Die Verwaltung der Systeme wird erleichtert, da diese ausgelagert wird. Die Verwaltung der Systeme wird aufgrund der Auslagerung und der erhöhten Dynamik erschwert.
- Je intensiver das Outsourcing verwendet wird, desto eher müssen Kontrollen (z.B. die Auftragskontrolle nach BDSG) und Notfallprozesse (z.B. Datenrückholung) an die neuen Prozesse angepasst werden.

# Mehr Informationen im Internet (Bsp.)

- BITKOM: [Leitfaden Cloud Computing](#)
- BSI: [Sicherheitsempfehlungen für Cloud Computing Anbieter](#)
- BMWi: [Themenseite Cloud Computing](#)
- ... oder fragen Sie uns!



Vielen Dank für Ihre Aufmerksamkeit!