

-

IT-Sicherheit im Mittelstand



Benedikt Auburger, VALEO IT

Alles CLOUDY???

- Was bedeutet Cloud Computing für die IT-Sicherheit im Mittelstand?
- Welche Auswirkung hat Cloud Computing für Anwender und Unternehmen?
- Welche Rolle spielt Sicherheit und Datensensibilität in der Cloud?

Die Cloud-Welle zielt seit geraumer Zeit nicht nur auf Business-to-Business (B2B), sondern auch auf Privatkunden . Im B2B Bereich ist Cloud Computing bereits teilweise anerkannt und wird von Unternehmen für spezielle nicht-geschäftskritische Services und Anwendungen eingesetzt. Sowohl für Unternehmen als auch Privatanwender stellt sich die Frage:

„Wie sicher sind meine Daten?“

- **Sogar Amazon S3 sei schon Opfer einer Attacke geworden. Wie US-Forscher vom MIT herausfanden, lassen sich Server von Cloud-Providern durchaus ausspionieren.**

Von wegen Cloud Computing ist absolut sicher.

Begriffe und Definitionen

- Cloud 3-Ebenenmodell:



Abb. Ebenen von Cloud Services nach IT-Leistungen und Zielgruppen

Begriffe und Definitionen

- EaaS:
 - Mittlerweile werden auch ganzheitliche Konzepte wie „Everything as a Service“ (EaaS) angeboten.
 - Dies beinhaltet unter anderem den Punkt „Human as a Service“ (HaaS), der den Support der Cloud-Anwendung für den Kunden bereitstellt
- Web services in the cloud
 - z. B. HP Reisekostenabrechnung

Organisationsformen



Private Cloud:

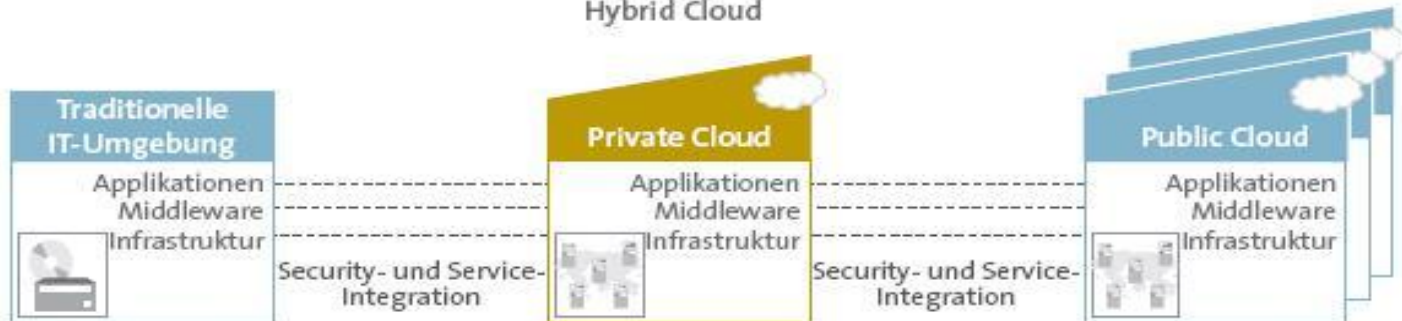
- Kundeneigene, vom Kunden selbst betriebene Cloud-Umgebung.
- Zugang beschränkt; nur für den Kunden selbst, autorisierte Geschäftspartner, Kunden und Lieferanten.
- Zugriff über Intranet
- Effiziente, standardisierte und sichere IT-Betriebsumgebung unter Kontrolle des Kunden, die individuelle Anpassung erlaubt.



Public Cloud:

- Im Eigentum eines IT-Dienstleisters befindliche und von diesem betriebene Cloud-Umgebung.
- Zugriff über Internet
- Flexible und schnelle Nutzung durch Subskription.
- Stellt eine Auswahl von hoch-standardisierten Geschäftsprozessen, Anwendungen und/oder Infrastrukturservices auf einer variablen "pay per use"-Basis zur Verfügung.

Hybrid Cloud



5 Cloud Charakteristiken von Mell und Grance (NIST)

- 1) Der Gedanke des „on-demand self-service“ ermöglicht dem User, ohne Interaktion mit dem Service-Provider, automatisch benötigte Ressourcen zu erwerben.
- 2) Wenn eine Anwendung zu Spitzenzeiten zusätzliche Ressourcen benötigt erfolgt diese automatisch durch „dynamische Skalierung“.

Bei Nichtauslastung werden nicht benötigte Ressourcen deaktiviert. Somit können Kosten sehr günstig gesteuert werden, da die Hardware immer perfekt ausgelastet ist.

5 Cloud Charakteristiken von Mell und Grance (NIST)

- 3) “Broad network access“ beschreibt den einfachen Zugang der Dienste über das Internet oder Intranet oder mobiler Endgeräte wie beispielsweise Smartphones, Laptops oder PDA’s.
- 4) “Resource Pooling“ beschreibt die Bündelung verschiedener Ressourcen eines Providers an einer Stelle, einem sogenannten Pool, der mehreren Benutzern zur Verfügung gestellt wird und welcher schließlich über einen Webservice zu erreichen ist.
- 5) Darüber hinaus sind Cloud Computing Systeme in der Lage die Zuteilung von Ressourcen vollkommen automatisch zu kontrollieren und zu optimieren

Technologieeinflüsse

- **Virtualisierung**
- **Webservices**
- **Service- orientierte Architekturen (SOA)**
- **Utility Computing**



Cloud Computing, IT-Management und IT-Sicherheit im Unternehmen

Die Einführung und Umsetzung von Prozessen in einer Cloud Umgebung erfordert die Unterstützung des IT-Managements und das Know-How der IT-Spezialisten. Der Aspekt der IT-Sicherheit spielt hier eine große Rolle, der bereits in der Planungs- und Konzeptionsphase des Projekts diskutiert und in der Umsetzung berücksichtigt werden soll.

Ausführungen zur IT-Sicherheit werden in diesem Kapitel erläutert und diskutiert.

Auswirkung auf die Anwender

- Keine „richtige“ lokale Software, sondern Web-Services oder Terminaldienste mit Authentifizierung (Single-Sign-On, PGP-Zertifikate,...)
- Frühzeitiges Einbinden der Anwender durch Flyer, Infoveranstaltungen und Schulungen erhöht die Akzeptanz
- Problembewältigung durch Bereitstellung eines geschulten IT-Supports (Hotline)

Auswirkung auf das Unternehmen

- Das IT-Management und das Team um den IT-Sicherheitsbeauftragten muss nach der Entscheidung für Cloud Computing, die grundlegenden Fragen diskutieren, welche ausgewählte Prozesse mit welchen Cloud Computing Technologien umgesetzt werden können.

Auswirkung auf das Unternehmen

- Meistens keine hohe Anschubfinanzierung notwendig
- Zusammenarbeit mit dem IT-Service-Dienstleister hinsichtlich der Projektierung und Umsetzung der Cloud Services
- Projektteam untersteht dem Management:
 - IT-Projektleiter
 - Fachabteilungs-Projektleiter
 - IT-Sicherheitsbeauftragter

Datensensibilität

- Diskussion der Sensibilität der auszulagernden Daten auf höchster Managementebene
- Es werden ausgereifte Prozesse ausgewählt um eine reibungslose Implementierung zu sichern
- Das IT-Management muss mit dem Anbieter der Cloud Dienste eine juristisch geprüfte vertragliche Regelung über den Datenzugriff treffen

IT-Sicherheitsstrategie für virtuelle Umgebungen erweitern

„Eine vom Sicherheitsunternehmen Shavlik in Auftrag gegebene Untersuchung zeigt, dass es für 80 Prozent der IT-Manager wichtig oder sogar kritisch ist, virtuelle Maschinen abzusichern.

Trotzdem gaben über 30 Prozent der Befragten Unternehmen an, keine Security-Tools im Einsatz zu haben, knapp 38 Prozent evaluieren derzeit Security-Tools. Nur 35 Prozent haben zur Absicherung ihrer virtuellen Umgebung Security- und Compliance-Tools im Einsatz.“

IT-Sicherheitsstrategie für virtuelle Umgebungen erweitern

Diese Untersuchung zeigt, dass eine Erweiterung und Überarbeitung der IT-Sicherheitsstrategie für ein Unternehmen, das virtuelle Umgebungen oder Cloud Dienste nutzen, dringend notwendig ist.

Hierzu zählen die Inventarisierung der virtuellen Umgebungen und deren Einsatzzweck um daraus eine IT-Sicherheitsstrategie abzuleiten.

Rollen und Zuständigkeiten

„Grundregeln bei der Definition von Rollen im Informationssicherheitsmanagement:

- Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung (und damit für die Informationssicherheit) verbleibt bei der Leitungsebene.
- Es ist mindestens eine Person (typischerweise als IT-Sicherheits-beauftragter) zu benennen, die den Informationssicherheitsprozess fördert und koordiniert.
- Jeder Mitarbeiter ist gleichermaßen für seine originäre Aufgabe wie für die Aufrechterhaltung der Informationssicherheit an seinem Arbeitsplatz und in seiner Umgebung verantwortlich.“

IT-Sicherheitsleitlinie

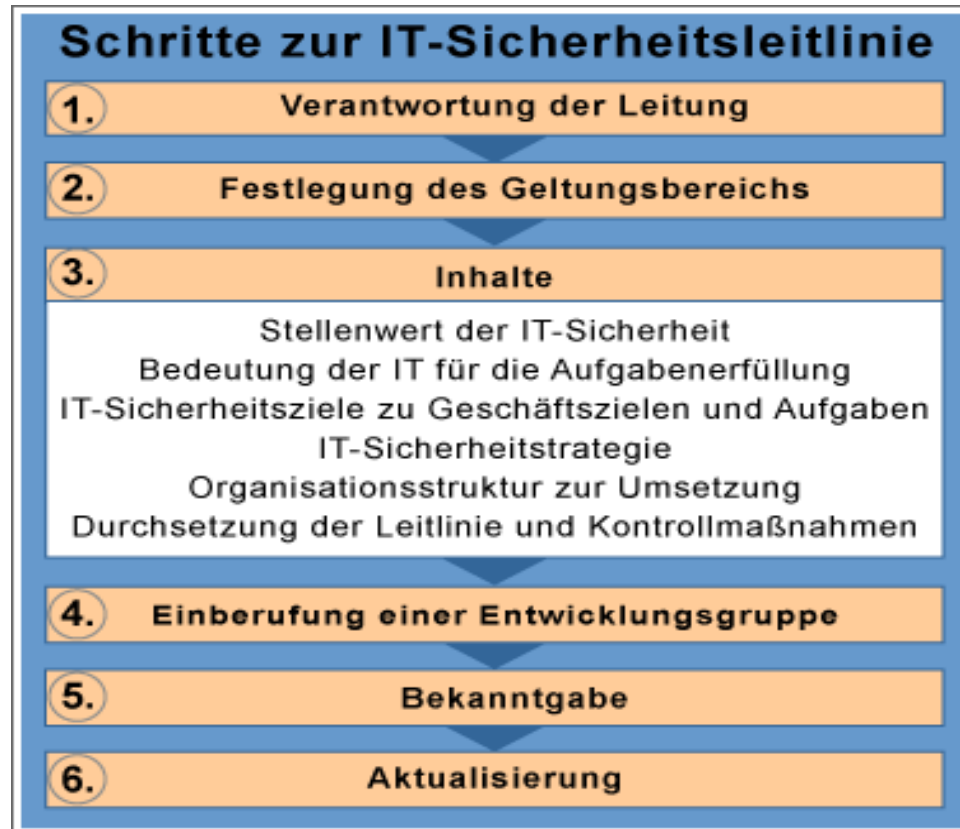


Abb. Schritte zur IT-Sicherheitsleitlinie des BSI

IT-Sicherheitskonzept

- Anpassen des IT-Sicherheitskonzepts an die Anforderungen des Cloud Computings.
- Hilfestellung bietet das BSI mit einer Grundschutzschulung oder der Anleitung für die Erstellung eines IT-Sicherheitskonzepts
- Prüfen, ob alle Punkte des eigenen IT-Sicherheitskonzepts bei dem Cloud-Anbieter umgesetzt werden

Risikoanalyse für Cloud Services

- Das Risiko für die Datensicherheit bei Cloud Services ist wesentlich höher als bei Nutzung der Daten in der Unternehmensinfrastruktur. Dies erfordert eine Risikoanalyse für die cloudbasierten Dienste. Dies soll mit dem Anbieter abgesprochen und vertraglich festgehalten sein, um spätere Komplikationen zu vermeiden.

Risikoanalyse für Cloud Services

- Eine Risikoanalyse beinhaltet:
 - eine ergänzende Sicherheitsanalyse
 - Erstellung der Gefährdungsübersicht
 - Ermittlung zusätzlicher Gefährdungen
 - Bewertung der Gefährdungen und Behandlung der Risiken.

Die Auslagerung von Business Intelligence Daten ist wesentlich kritischer zu bewerten als die Nutzung von Cloud Computing in der Reisekostenabrechnung.

Vertragsrechtliche Details

- Eine Weitergabe von Unternehmensdaten erfordert eine juristische Absicherung für Anbieter und Kunden der Cloud Dienste.
- In einem Vertrag sollte festgehalten sein, wer für Schäden am Kunden haftbar ist.
- „Private Clouds erscheinen etwa aus rechtlicher Sicht wenig problematisch, stellen sie doch lediglich eine unternehmensinterne technische Reorganisation von IT-Strukturen ohne Auswirkungen auf vertragliche Außenbeziehungen dar.
- Werden solche Private Clouds von Dritten betrieben, liegt aus rechtlicher Sicht ein klassisches IT-Outsourcing vor.“

Vertragsrechtliche Details

- Für das Betreiben einer Public oder Hybrid Cloud, empfiehlt die Bitkom im Flyer „Cloud Computing“. Es sollten:
 - Standardisierung
 - Mandantenfähigkeit
 - Kombinierbarkeit
 - Skalierbarkeitals rechtliche Bestandteile im Vertrag aufgeführt sein.

Datenschutz und Datensicherheit

- Der IT-Grundschatz Katalog des BSI erklärt Datenschutz folgend:
 - „Aufgabe des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen ("informationelles Selbstbestimmungsrecht").“
 - Das Unternehmen, das Cloud Computing nutzt, muss seine Mitarbeiter mit Hilfe des Datenschutzbeauftragten über Datenschutz in der Cloud aufklären. Die Datensicherheit in der Cloud muss vom Anbieter im Sinne der vertraglichen Regelung hergestellt und gewährleistet werden.

Kriterien zur Einordnung von Cloud-Anbietern

- Die Bereitstellung der Services im Self-Service-Modell soll den Gedanken der Selbstbedienung und „On-Demand“ unterstreichen. Lediglich ein Mausklick soll den Benutzer dazu befähigen, den ausgewählten Dienst aus der Cloud zu abonnieren.
- Der Zugriff über IP-Netze soll ebenso erfolgen, egal wo der Benutzer den Dienst anfordert oder mit welcher Hardware.

Kriterien zur Einordnung von Cloud-Anbietern

- Ein Kriterium ist die hohe Skalierung von Anwendungen oder Infrastrukturleistungen. Der Service-Provider soll hierbei in der Lage sein, Lastspitzen mit Ressourcen zu versorgen, um eine Stabilität des Dienstes zu schaffen. Ebenso bei niedriger Auslastung soll der Anbieter für eine optimale Anpassung der Ressourcenbereitstellung sorgen.
- Das Bezahlmodel „Pay-As-You-Go“ (Zahlen nach abgerechneter Leistung) soll dem Kunden eine nutzengerechte Abrechnung gewährleisten. Es erfolgt eine Bezahlung der Ressourcen oder Leistungen, die der Kunde in Anspruch nimmt. Andere Bezahlmodelle, wie monatliche Abrechnung von Service-Leistungen bieten Anbieter ebenfalls an, welche im Unterschied zu „pay-as-you-go“ für den kompletten Monat gebucht werden.

Kriterien zur Einordnung von Cloud-Anbietern

- Cloud Computing basiert in erster Linie auf verschiedenen Visualisierungstechniken.
- Abstrahierte und virtualisierte Infrastrukturen von Anbietern sollen darüber hinaus eine standardisierte Auslieferung rechtfertigen.

Compliance-Anforderungen

- Compliance-Anforderungen des Kunden und gesetzliche Regelungen für spezifische Daten setzen zusätzliche Kriterien für die IT-Sicherheit.

Die Umsetzung erfordert nicht nur die Analyse und Bewertung der Sicherheitsmaßnahmen des Providers durch den Kunden. Notwendige Maßnahmen sind **vor Beginn der Nutzung** der Cloud-Lösung zu vereinbaren und zu realisieren.

Sicherheitsrisiken

- Ungenügende Mandantentrennung
 - Bei nicht ausreichend abgesicherter Mandantentrennung besteht die Gefahr, dass Dritte unauthorisiert Daten einsehen oder manipulieren können. Dieses Risiko ist in einer Public Cloud erhöht, da durch Virtualisierung und Grid Computing keine physikalische Trennung der Daten unterschiedlicher Mandanten erfolgt.

Sicherheitsrisiken

- Verletzung der Compliance
 - Da Daten in einer Public Cloud prinzipiell in allen Ländern der Welt in deren spezifischen Rechtsordnungen verarbeitet werden können, ist die Erfüllung aller gesetzlicher Anforderungen eine wesentliche Aufgabe bei der Nutzung von Public Cloud Leistungen.

Sicherheitsrisiken

- Verletzung von Datenschutzgesetzen
 - Es ist nicht von vornherein klar, in welchen Ländern, Rechenzentren, auf welchen Servern und mit welcher Software die Daten gespeichert und verarbeitet werden. Auch sind die Datenflüsse unbekannt. Es besteht dadurch die Gefahr der Verletzung von Datenschutzvorschriften.

Sicherheitsrisiken

- Handel mit Ressourcen wird denkbar
 - Denkbar ist auch, dass Provider einen Handel mit ihren Ressourcen untereinander aufbauen und damit eine "Ressourcenbörse" realisieren. Auf dieser Börse werden Ressourcen zu einem bestimmten Preis angeboten. In Leistungsspitzen würde etwa der Preis pro CPU Stunde auf der Börse höher gehandelt. Welche Konsequenzen dies für die Sicherheit der Daten haben kann, ist noch vollkommen unklar.

Vorgehensweise

- **1. Planungsphase**
- **2. Vertragsphase**
- **3. Migration**
- **4. Betriebsphase**
- **5. Beendigung der Auslagerung**

1. Planungsphase

- Die Auslagerung in die Public Cloud wird einer Sicherheits- und Risikoanalyse unterzogen
- Zudem wird ermittelt, welche gesetzlichen (insbesondere des Datenschutzes) und organisatorischen Anforderungen für die Auslagerung gelten
- Aus all diesen Informationen werden die zu erfüllenden "Sicherheitsanforderungen" abgeleitet
- Es wird ein Leistungskatalog erstellt, der detailliert die Auslagerung und alle geforderten Leistungen inklusive aller Sicherheitsanforderungen beschreibt

2. Vertragsphase

- Ziel ist es, in Verträgen und/oder Service Level Agreements (SLA) eine vollständige und kontrollierbare Leistungsbeschreibung zur Gewährleistung der Qualität und Informationssicherheit in der Public Cloud zu vereinbaren.

2. Vertragsphase

- Einräumung von Auditrechten für Dokumente, Beschreibungen und Protokolle
- Definition messbarer Kennzahlen für Vertraulichkeit und Integrität
- Schnittstellendefinition für Security Monitoring und Incident Handling
- Regelungen für die Beendigung der Cloud-Leistungen (Datenübergabe und Datenlöschung)

3. Migration

- Nach Vertragsabschluss beginnt die schrittweise und geplante Migration. Zur Planung gehört die Erstellung von Sicherheitskonzepten, die sowohl die Migration als auch den Betrieb und die Beendigung der Auslagerung beinhalten.
- Als Basis für die Erstellung dienen die Ergebnisse der Risikoanalyse. Die Umsetzung und das Testen der Auslagerung in die Cloud erfolgen nach den erstellten Sicherheitskonzepten.

4. Betriebsphase

- Während der Betriebsphase werden die ausgelagerten Funktionen gemäß Vertrag und Sicherheitskonzepten durch den Provider betrieben.
- Wichtig ist ein Security Monitoring, um Abweichungen vom erforderlichen Sicherheitsniveau erkennen zu können. Das Security Monitoring dient auch dazu, die Erfüllung der vereinbarten Leistungen nachweisen, kontinuierlich verbessern und überprüfen zu können.

5. Beendigung der Auslagerung

- Die Beendigung muss nach den vertraglich vereinbarten Regelungen erfolgen.
- Der Provider muss insbesondere Daten auf seinen Systemen nachweisbar so löschen, dass sie auch mit ausgefeilten Methoden und Technologien nicht wiederherstellbar sind.
- Hierzu zählen nicht nur Daten des Geschäftsprozesses, sondern auch betriebliche Daten wie Protokolldaten von Systemen und Applikationen.

Provider-Sicherheit

- Es liegt bereits im eigenen Interesse der Provider, Sicherheitsmaßnahmen zu implementieren, die das Niveau vieler Anwender deutlich übertreffen.
- Kunden können diese Maßnahmen für ihr eigenes Sicherheitskonzept nutzen, wenn sie entsprechende Maßgaben zuvor im Cloud-Computing-Vertrag vereinbaren.

Fazit

- Sicherheit und Cloud Computing schließen sich nicht gegenseitig aus, erfordern aber ein hohes Maß an Sensibilität in der IT-Sicherheit.
- Die Planung und Umsetzung von IT-Sicherheitsmaßnahmen soll das Unternehmen bereits vor der Inbetriebnahme der Cloud mit Hilfe der IT-Abteilung und dem Cloud Dienstleister realisieren.

Ende des Vortrags & Diskussion

