Security in der Cloud
Ein Leidfaden für Fragen an Anbieter von Cloud Services.

Cloud IT ist bereits auf dem Weg zum Mainstream. Bis 2014 werden weltweit 40% neuer Anwendungen in Cloud-Lösungen investiert, 25% der gesamten Workload wird dann in der Cloud stattfinden.

Die entstandene Diskussion über Datensicherheit und Datenschutz in der Cloud hat in letzter Zeit sehr stark an Bedeutung gewonnen und ist zu einem wichtigen Kritikpunkt geworden.
IT Executives, die planen, Cloud Services einzusetzen, sollen proaktiv Anbieter über Datensicherheit, sowohl nach traditionellen wie nach Multi-Instance Aspekten anfragen. Dies sind legitime Bedenken wie Ansprüche, die von Anbietern wie von Anwendern zu adressieren sind.

Die aufgeführten Fragen dienen daher in erster Linie einer fachlichen Auseinandersetzung und Versachlichung.

- **Fachliche Anforderungen oder Voraussetzungen.**
  Haftungsfragen, vertragliche Abmachungen, Laufzeiten, Konditionen und SLAs (Service Level Agreements), sind ohne Zweifel der umfangreichste wie komplexeste Teil der Cloud-Nutzung, sind aber im eigentlichen Sinn nicht sicherheitsrelevant. Soweit Datensicherheits-Aspekte betroffen sind, sollten diese Fragen gestellt werden:

  Wie kann der Kunde auf seine Daten zugreifen oder diese wiederherzustellen. Wie wird Sicherung der Daten einschließlich Disaster Recovery gewährleistet?

  Wie, in welchem Format und nach welchen Umständen oder Bedingungen werden bei Vertragsende die Daten des Kunden an ihn übergeben?

- **Technische Anforderungen zur Sicherstellung von Datenschutz und -sicherheit.**
  Dieser umfangreiche Komplex dient einer Übersicht, nicht alle Fragen sind für alle Nutzungsfälle relevant.
  Sind die Rechenzentren uneingeschränkt, 24h x 7 Tage physikalisch, auch nach Mehr-Personen-Prinzip, gesichert?

  Ein äußerst wichtiger Teil umfasst die Benutzer-Identifikation und deren Schutz. Ist es sichergestellt, dass der Provider, bzw. sein Personal keinen Zugang zu Benutzerpasswörter oder Berechtigungen des Anwenders hat, oder diese einsehen kann?

  Existieren dokumentierte Vorschriften zu Passwortrichtlinien, Zugriffsbeschränkungen, Anmeldeprotokollierungen, Datenzugriffsmodellen und Feldebenenzugriffskontrollen)

  Ist es gewährleistet, dass alle Passwörter verschlüsselt sind und sicheres Session Key Management und Multi-Tenant Datenzugriffskontrolle bestehen?

  Werden Sicherheitsverstöße überwacht?

- **Transaktion im Internet**
  Wird 128-bit SSL Verschlüsselung für jede Transaktion vorgenommen und liegen Verisign Zertifikate vor?

  Sind ständig überwachte Perimeter Firewalls, Intrusion Detection- und proaktives Log-File-Monitoring Standard-Verfahren?

- **Sicherheitsmonitoring**
  Wird ein Monitoring erfolgreicher/fehlgeschlagener Logins, SU-Änderungen, wie ständiges Perimeter-, Third Party-Monitoring von Domain-Namen und SSL-Zertifikaten durchgeführt?

  Werden Intrusion Detection und Security Event Management dokumentiert?

- **Interoperabilität von Security-Architekturen von Cloud Services zu eigenen, On-Premise-Anwendungen.**
  Cloud IT ist in vielen Fällen für Anwender Teil einer Lösung. Cloud IT wird häufig mit internen Systemen verbunden oder interagiert mit diesen (hybrider Ansatz).

  In welcher Weise haben Security-Architekturen und -Praktiken des Anbieters Einfluss in der Verbindung zu On-Premise-Systemen des Kunden?

  Sind Multi-Tenancy und virtualisierter SaaS/Cloud-Plattform-Umgebungen bezogen auf Data-Partitioning-Technologien und -Praktiken, offenlegt und dokumentiert (ISO 15408)?

- **Gesetzliche oder durch Verordnungen verfügte Anforderungen (BDSG), soweit die Cloud Services personenbezogene Daten vorhalten oder verarbeiten.**
  Gemäß Paragraf 4b Absatz 2 Satz 2 BDSG setzt die Übermittlung personenbezogener Daten in einen Drittstaat voraus, dass dieser ein angemessenes Schutzniveau gewährleistet. Sollten die gesetzlichen Regelungen dies gewährleisten, ist noch zu fragen, ob das jeweilige Unternehmen den gesetzlichen Normen Folge leistet oder nicht.

  Ist bei Speicherung von personenbezogenen Daten außerhalb der Grenzen des Europäischen Wirtschaftsraumes ein angemessenes Schutzniveau gewährleistet?

  Eine Herausforderung stellt die hohe Internationalisierung/Globalisierung der Clouds dar. Deshalb sollte bei der Vertragsgestaltung Augenmerk auf die Wahl des Gerichtsstands und des anzuwendenden Rechts gelegt werden. Trotz der freien Wahl des Rechts und des Gerichtsstands ist jeweils das zwingende Recht in dem Land zu berücksichtigen, wo sich die Daten oder einer der Vertragsparteien befinden. Deshalb bedarf es rechtlicher Konzepte, die diesen erhöhten Anforderungen gerecht werden (Datenschutz nach dem Safe-Harbor-Prinzip).

  Ist es sichergestellt, dass die zur Nutzung einer Anwendung Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogenen Daten bei der Verarbeitung, Nutzung und nach Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können?

  Ist es gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Anwendungs-Systeme eingegeben, verändert oder entfernt worden sind?

  Ist es gewährleistet, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können?

Zusammenfassend, Cloud Computing ist unaufhaltsam und für Agilität und Wettbewerbsfähigkeit ohne Alternative. Vorausschauende Unternehmen sehen das Management und den Umgang mit den Risiken der Cloud daher als eine Herausforderung an.

Frank P. Sempert
Senior Program Executive, Europe
Saugatuck Technology, Inc.
E-Mail:
frank.sempert@saugatucktechnology.com