IT-Grundschutz und Cloud Computing

Alex Didier Essoh

Bundesamt für Sicherheit in der Informationstechnik

SECMGT Workshop Cloud Computing
20.11.2009

Agenda

- Was ist IT-Grundschutz?
- Was ist Cloud Computing?
- Was ist aus Sicht der Informationssicherheit zu beachten?
- Zusammenfassung

BSI-Standard 100-1,2,3,4
BSI-Standards zur Informationssicherheit

BSI-Standards
- Bereich IS-Management -

BSI Standard 100-1:
ISMS: Managementsysteme für Informationssicherheit

BSI Standard 100-2:
IT-Grundschutz-Vorgehensweise

BSI Standard 100-3:
Risikoanalyse auf der Basis von IT-Grundschutz

BSI Standard 100-4:
Notfallmanagement

Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

IT-Grundschutz-Kataloge

Kapitel 1: Einleitung

Kapitel 2: Schichtenmodell und Modellierung

Kapitel 3: Glossar

Kapitel 4: Rollen

- **Bausteinkataloge**
  - Kapitel B1 Übergreifende Aspekte
    - B 1.0 Sicherheitsmanagement
    - ...
  - Kapitel B2 Infrastruktur
  - Kapitel B3 IT-Systeme
  - Kapitel B4 Netze
  - Kapitel B5 IT-Anwendungen
- **Gefährdungskataloge**
- **Maßnahmenkataloge**

Dienstleistungen und Produkte rund um den IT-Grundschutz

Sicherheitsbedarf, Anspruch

- -
- °
- +

Leitfaden Informationssicherheit

Webkurs zum Selbststudium

BSI Standard 100-1: ISMS

Hilfsmittel & Musterrichtlinien

Software: „GSTOOL“

BSI Standard 100-2: IT-Grundschutz-Vorgehensweise

Beispiele: „GS-Profile“

ISO 27001-Zertifikat

BSI Standard 100-3: Risiko-Analyse

IT-Grundschutz-Kataloge

Leitfaden IS-Revision

BSI Standard 100-4: Notfall-management

BSI-Empfehlungen:
- Internetsicherheit
- Hochverfügbarkeit

Agenda

- Was ist IT-Grundschutz?
- Was ist Cloud Computing?
- Was ist aus Sicht der Informationssicherheit zu beachten?
- Zusammenfassung

Zitate

- A lot of people are jumping on the cloud bandwagon, but I have not heard two people say the same thing about it. There are multiple definitions out there of „**the cloud**“.

  Quelle: HP Vice President of European Software Sales (ESS) Andy Isherwood, quoted ZDNews, Dec 11, 2008

- The interesting thing about Cloud Computing is that we've redened Cloud Computing to include everything that we already do. . . . I don't understand what we would do differently in the light of Cloud Computing other than change the wording of some of our ads.

  Quelle: Oracle CEO Larry Ellison, quoted in Wall Street Journal, Sept 26, 2008

Was ist Cloud Computing?

- Von Cloud Computing wird dann gesprochen, wenn eine oder mehrere der folgenden drei IT-Dienstleistungen
  - Infrastruktur (Rechenleistung, Hintergrundspeicher, etc.)
  - Plattform
  - Anwendungssoftware

  aufeinander abgestimmt, schnell und dem tatsächlichen Bedarf angepasst sowie nach tatsächlicher Nutzung abrechenbar über ein Netz bereitgestellt werden.
- 5 Charakteristiken
- 3 Bezugsmodelle
- 4 Geschäftsmodelle

Was ist charakteristisch für Cloud Computing?

- Abstraktion der Infrastruktur
- Demokratisierung der Ressourcen
- (Dienstorientierte Architektur)
- Elastizität / Dynamismus
- Utility Model

Quelle: Cloud Security Alliance (CSA)

Wie wird Cloud Computing ausgeliefert?

- Software as a Service (SaaS)
  - Anwendungen werden über ein Netz bereitgestellt
  - Beispiele: Google Apps (Gmail, Docs, etc.), CRM-Salesforce.com
- Platform as a Service (PaaS)
  - Entwicklungsumgebungen werden über ein Netz bereitgestellt
  - Beispiele: Windows Azure Platform, Google App Engine, Force.com
- Infrastructure as a Service (IaaS)
  - Virtuelle Server, Hintergrundspeicher, Load Balancer, etc. werden über ein Netz zur Verfügung gestellt
  - Beispiele: Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), Serve Path Gogrid

Was sind die Geschäftsmodelle?

	Managed by	Infrastructure owned By	Infrastructure Located	Accessible and Consumed by
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Managed	Third Party Provider	Third Party Provider	On-Premise	Trusted or Untrusted
Private	Organisation Third Party Provider	Organisation Third Party Provider	On-Premise Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organisation & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

Quelle: Cloud Security Alliance (CSA)

Wer nutzt die Cloud?

- Stadtverwaltung Washington D.C. (38.000 Angestellte)
  - Google Apps (Gmail, Google Docs, Google Video, Google Sites)
- Stadtverwaltung Kalifornien (30.000 Angestellte)
  - Gmail wird ab Mitte 2010 eingesetzt
- General Electric
  - 400.000 Destops (Zoho)
- New York Times
  - nutzte Amazon EC2 und S3, um 11 Millionen Artikel für das Online-Archiv in PDFs zu konvertieren
  - 100 VM-Instanzen wurden gemietet und die Konvertierung dauerte 24 Stunden

Was sind die Gründe für die Nutzung?

- Flexibilität bei der Buchung, Nutzung und Stilllegung von Rechenzentrenkapazitäten je nach aktuellem und ggf. auch nur kurzfristigem Bedarf
- Einfacher Erwerb, verbrauchsabhängige Bezahlung
- Einsparpotential im Bereich
  - Anschaffung, Betrieb und Wartung der IT-Systeme
- Ubiquitäre Verfügbarbeit von Geschäftsanwendungen unabhängig vom geografischen Standorten

Agenda

- Was ist IT-Grundschutz?
- Was ist Cloud Computing?
- Was ist aus Sicht der Informationssicherheit zu beachten?
- Zusammenfassung

Sicherheitsanalyse von Cloud Computing

Vorgehensweise

- Festlegung der Schutzziele
  - Vertraulichkeit, Integrität und Verfügbarkeit
- Identifizierung der zu schützenden Zielobjekte
  - Daten und Anwendungen in der Cloud
  - Behörden-/Unternehmensnetz
- Erarbeitung von Sicherheitsmaßnahmen

Gefährdungen

- Fehler/Angriffe durch Mitarbeiter der Provider
- Angriffe durch andere Kunden der Cloud
- (Angriffe auf die Verfügbarkeit)
- Fehler bei der Provisionierung und beim Management
- Missbrauch der Provider-Plattform
- Web-Service basierte Angriffe

Provider Mitarbeiter

Gefährdungen

- Unberechtigtes Kopieren einer VM
- Modifikation einer VM nach deren Erzeugung
- Herunterfahren einer VM
- Herunterfahren eines Hosts
- Unbeabsichtiges Löschen von Daten
- Dekonnektierung wichtiger Netzelemente
- Manipulation von Konfigurationsdateien

Maßnahmen

- Schulung, vor allem für Sicherheitsaspekte
- Audits durchführen beim Provider
- Trennung der Funktionen und Rollen
- Sicherheiheitsrichtlinien

Angriffe durch andere Kunden

Gefährdungen

- Übernahme der Kontrolle über andere VM
- Zugriff auf das Dateisystem des Hosts
- DoS auf den Hypervisor
- Abhören der Kommunikation zwischen den VMs
- Unberechtigter Zugriff auf Daten im Speicher

Maßnahmen

- Einsatz von sicheren Hypervisoren
- Trennung der Netze durch den Einsatz von VPN, VLANs und Firewall
- Einsatz starker Kryptographie
- Trennung der Daten

Angriffe auf die Verfügbarkeit

Gefährdungen/Schwachstellen

- Software-Fehler aufgrund der Komplexität der Plattformen
- DDoS-Angriffe beispielsweise durch Botnetze
- Ausfall der Verbindung zwischen Provider und Kunde (Single Point of Failure)
- Verfügbarkeit der Anwendungen beim Patchen

Maßnahmen

- Sichere Software-Entwicklung
- DDoS-Mitigation
- Redundanz schaffen, beispielsweise durch einen zweiten Provider
- Verfügbarkeit des Providers monitoren

Missbrauch der Cloud-Plattform

Gefährdungen

- Durchführung von Brute-Force Angriffen auf Passwörter
- Aufbau von Botnetzen
- Ablage für Schadsoftware
- Versenden von SPAM

Maßnahmen

- Network Intrusion Detection
- Scannen der Inhalte nach Schadprogrammen
- Filterung von bösartigen E-Mails

Provisionierung und Management

Gefährdungen

- Unsichere Images
- Rechenfehler bei der Reservierung von Ressourcen
- Ausfall des Provisioning Manager
- Manipulation von Konfigurationsdateien
- Konfigurationsfehler
- Fehler beim Upgrade der Systeme

Maßnahmen

- Qualitätsmanagement
- Redundanz schaffen
- Patch- und Konfigurationsmanagement

Web-Anwendungen

Gefährdungen

- Webservice-basierte Angriffe wie z.B.
  - Malicious Software Angriffe
  - Identity und Identity Service Spoofing
  - SOAP Flooding Angriffe
  - Angriffe auf das XML Parsing System
  - etc.

Maßnahmen

- Sichere Software-Entwicklung
  - siehe BSI-Studie Sicherheit von Webanwendungen
  - siehe BSI-Studie SOA-Security Kompendium, Version 2.0

Weitere kritische Bereiche von Cloud Computing

- ID-Management
- Schlüsselmanagement
- Compliance
- Interoperabilität der Plattformen
- Portabilität der Daten und Anwendungen
- Notfallvorsorge
- Verlässlicheit des Providers

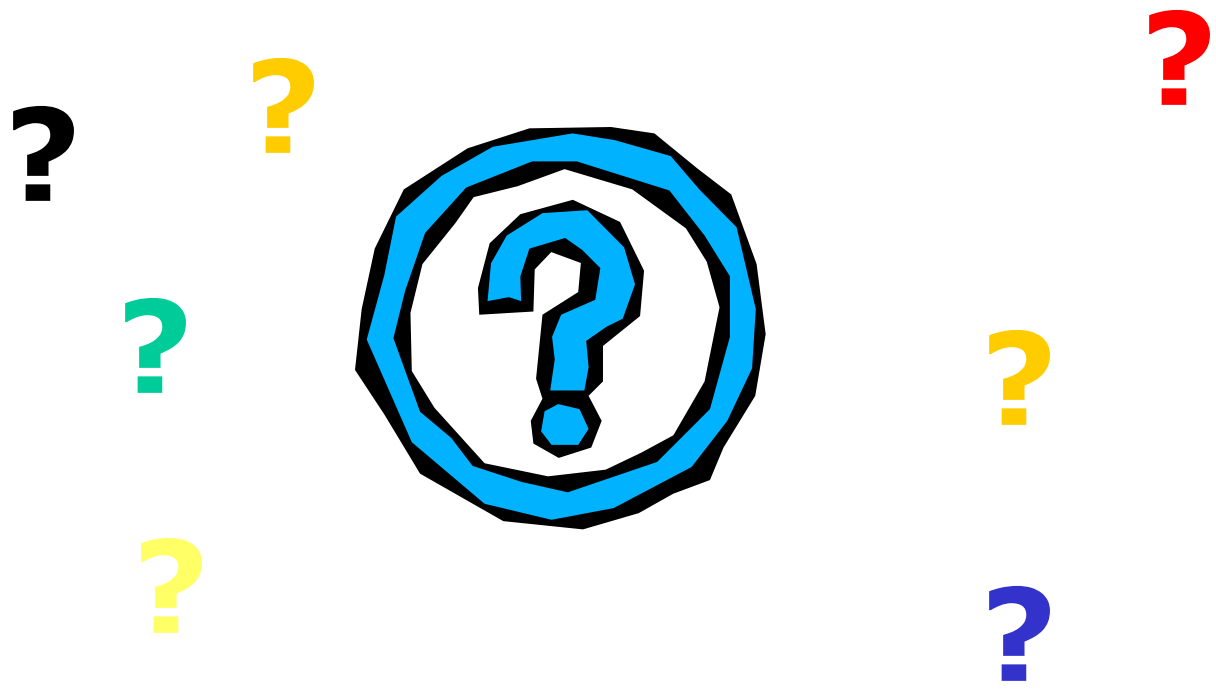
Empfehlungen des BSI

- Kleine und mittlere Unternehmen können durch den Einsatz von Cloud Computing ihre Sicherheit verbessern.
- Firmen, die Cloud Computing nutzen wollen, müssen sich ihre Sicherheitsanforderungen in Abhängigkeit vom Schutzbedarf der Daten vom Betreiber vertraglich zusichern lassen, einschließlich eines Revisionsrechtes.
- die Nutzung von Cloud Computing ist einer Risikoabwägung zu unterziehen.

BSI-Planung

- Mittelfristig plant das BSI verschiedene Veröffentlichungen zum Thema Cloud Computing
  - Anforderungen an Provider
  - Empfehlungen für Benutzer

Fragen und Diskussionen



Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Alex Didier Essoh
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)228-99-9582-5391
Fax: +49 (0)228 99 10 9582 5391

alex.essoh@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de