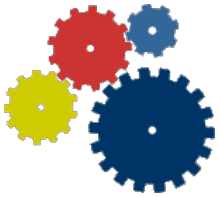
Bundesamt
für Sicherheit in der
Informationstechnik

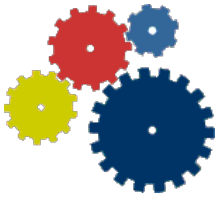


BSI-Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter

Alex Didier Essoh und Dr. Clemens Doubrava

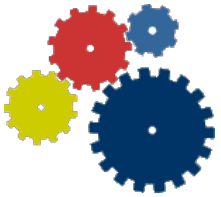
EuroCloud Deutschland_eco e.V. – Köln – 02.02.2011

Ziel



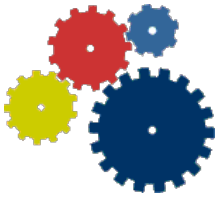
- Ziel des BSI ist es, gemeinsam mit den Marktteilnehmern (Anbieter und Anwender) sachgerechte Sicherheitsanforderungen an Cloud Computing zu erarbeiten
- Das Papier wurde am 28.09.2010 in der Version 0.96 auf der BSI-Webseite veröffentlicht
- Das Eckpunktepapier wurde konstruktiv kommentiert
- Beiträge fließen in die finale Version der BSI-Mindestsicherheitsanforderungen ein

Eckpunkte



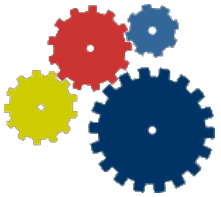
- Sicherheitsmanagement beim Cloud-Anbieter
- Sicherheitsarchitektur
- ID- und Rechtemanagement
- Monitoring und Security-Incident Management
- Notfallmanagement
- Sicherheitsprüfung und -nachweis
- Anforderungen an das Personal
- Transparenz
- Organisatorische Anforderungen
- Kontrollmöglichkeit für Nutzer
- Portabilität von Daten und Anwendungen
- Interoperabilität
- Datenschutz/Compliance
- Cloud-Zertifizierung
- Zusatzforderungen/ Bundesverwaltung

1. Sicherheitsmanagement beim Anbieter



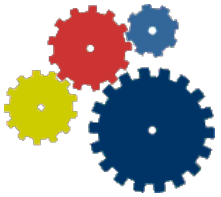
- Jeder Betreiber einer Cloud-Computing-Plattform muss **ein wirksames ISMS** (Information Security Management System) wie beispielsweise nach ISO 27001 oder bevorzugt IT-Grundschutz auf Basis von ISO 27001 umsetzen
  - Definiertes Vorgehensmodell aller IT-Prozesse (z. B. nach ITIL, COBIT)
  - Implementation eines anerkannten Informationssicherheits-Managementsystems (z. B. BSI-Standard 100-2 (IT-Grundschutz), ISO 27001)
  - Erstellung eines IT-Sicherheitskonzeptes für die Cloud

2. Sicherheitsarchitektur



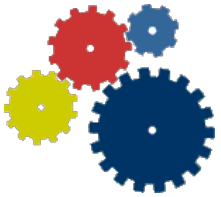
- Jeder Cloud-Anbieter muss eine durchgängige **Sicherheitsarchitektur** konzipieren und implementieren
  - Rechenzentrumssicherheit
  - Netzsicherheit
  - Host- und Servervirtualisierung
  - Anwendungs- und Plattformsicherheit
  - Datensicherheit
  - Verschlüsselung und Schlüsselmanagement
  - .....
- Darüber hinaus müssen die eingesetzten Cloud-Computing-Plattformen **mandantenfähig** sein und eine verlässliche Trennung der Mandanten gewährleisten

3. ID- und Rechtemanagement



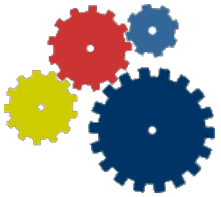
- Die Identitätsverwaltung muss von jeder Cloud-Plattform unterstützt werden
  - Starke Authentisierung (z. B. Zweifaktor-Authentisierung) für Administratoren des Cloud-Anbieters
  - Starke Authentisierung (z. B. Zweifaktor-Authentisierung) für Cloud-Nutzer
  - Least Privilege Model (Nutzer bzw. Administratoren sollen nur die Rechte besitzen, die sie zur Erfüllung ihrer Aufgabe benötigen)
  - Vier-Augen-Prinzip für kritische Administrationstätigkeiten

4. Monitoring und Security-Incident Management



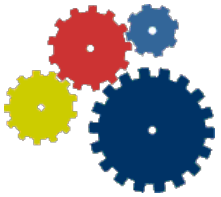
- Jeder Cloud-Anbieter muss ein **wirksames Monitoring** implementieren und dem **Cloud-Nutzer aussagekräftige Monitoringdaten zur Verfügung stellen**
  - 24/7 Überwachung der Cloud
  - Einbindung in die CERT-Strukturen und das nationale IT-Krisenmanagement
  - Erkennung von internen Angriffen von Cloud-Nutzern auf andere Cloud-Nutzer
  - Logdatenerfassung und Auswertung
  - 24/7-erreichbares und handlungsfähiges Cloud-Management und Trouble-Shooting

5. Notfallmanagement



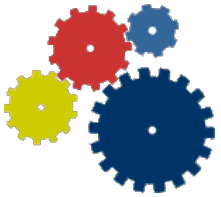
- Jeder Cloud-Anbieter muss über ein **Notfallmanagement** verfügen, basierend auf etablierten Standards wie beispielsweise BS 25999 oder BSI-Standard 100-4
  - Implementierung eines Notfallmanagements
  - Regelmäßige Übungen
  - Nachweis eines implementierten Notfallmanagements (beispielsweise auf Basis von BS 25999 oder BSI-Standard 100‑4)

6. Sicherheitsprüfung und -nachweis



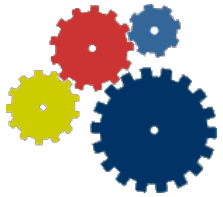
- Der Cloud-Anbieter muss regelmäßig den **IT-Sicherheitszustand** überprüfen lassen und entsprechende **Prüfnachweise** den Cloud-Nutzern zur Verfügung stellen
  - Der Cloud-Anbieter muss dem Cloud-Nutzer regelmäßig berichten
  - Regelmäßige Penetrationstests
  - Regelmäßige Penetrationstests bei Subunternehmen
  - Regelmäßige und unabhängige Sicherheitsrevisionen
  - Regelmäßige und unabhängige Sicherheitsrevisionen bei Subunternehmern

7. Anforderungen an das Personal



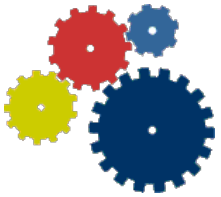
- Der Cloud-Anbieter muss sicherstellen, dass sein **Personal vertrauenswürdig, geschult und auf definierte Regeln verpflichtet ist**
  - Vertrauenswürdiges Personal
  - Ausbildung der Mitarbeiter des Cloud-Anbieters (Regelmäßige Schulung)
  - Sensibilisierung der Mitarbeiter des Cloud-Anbieters für Informationssicherheit und Datenschutz
  - Verpflichtung der Mitarbeiter auf Datenschutz, Sicherheitsmaßnahmen, Vertraulichkeit der Kundendaten

8. Transparenz



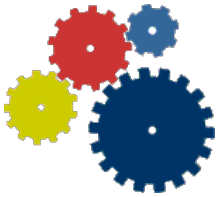
- Der Cloud-Anbieter **muss offen legen**, an welchen Standorten die Daten und Anwendungen gespeichert und verarbeitet werden und wie dort der Zugriff durch Dritte geregelt ist
  - Offenlegung der Standorte des Cloud-Anbieters (Land, Region)
  - Offenlegung der Subunternehmer des Cloud-Anbieters
  - Transparenz, welche Eingriffe der Cloud-Anbieter in Daten und Verfahren der Kunden vornehmen darf
  - Regelmäßige Unterrichtung über Änderungen (z. B. neue oder abgekündigte Funktionen, neue Subunternehmer, andere Punkte, die für das SLA relevant sind)
  - Transparenz über staatliche Eingriffs- und Einsichtrechte
  - Darlegung der Rechts- und Besitzverhältnisse des Cloud-Anbieters sowie der Entscheidungsbefugnisse

9. Organisatorische Anforderungen



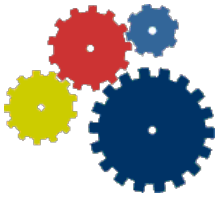
- Sicherheitsleistungen müssen zwischen dem Cloud-Anbieter und dem Cloud-Nutzer vertraglich vereinbart werden, **vorzugsweise in einem Security-SLA oder an hervorgehobener Stelle im SLA**.
  - Definierte Sicherheitsleistungen durch Security-SLA oder im SLA deutlich hervorgehoben
  - Einsicht in Security-SLA bzw. SLA von Subunternehmern
  - Rahmenbedingungen zur Gültigkeit des SLAs aufführen (z. B. keine Verpflichtung zur Leistungserbringung aufgrund Höherer Gewalt)
  - Sicherstellung des Betriebs oder der Bereitstellung der Daten im Falle einer Insolvenz des Cloud-Anbieters

10. Kontrollmöglichkeiten für Nutzer



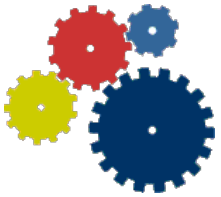
- Den Cloud-Nutzern muss es möglich sein, **Audits beim Cloud-Provider** durchzuführen. Hierfür kann der Cloud-Anbieter Schnittstellen zur Verfügung stellen. Sofern dies nicht möglich ist, muss der Cloud-Anbieter dem Nutzer äquivalente, **durch Dritte erstellte Auditberichte** vorlegen
  - Kunden sollen die Möglichkeit haben die Einhaltung der SLAs zu überwachen, indem beispielsweise die Qualität der angebotenen Services überwacht wird
  - Durchführung eines Audits beim Cloud-Anbieter durch den Cloud-Nutzer
  - Möglichkeit des Kunden, in Abstimmung mit dem Anbieter, Penetrationstests durchzuführen

11. Portabilität von Daten und Anwendungen



- Cloud-Dienste müssen so gestaltet sein, dass der Cloud-Nutzer seine Daten jederzeit aus der Cloud wieder exportieren kann (**kein vendor lock-in**)

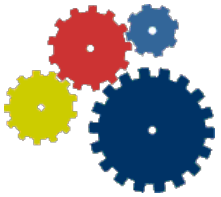
12. Interoperabilität



- Die Interoperabilität von Cloud-Computing-Plattformen definiert die Fähigkeit, unabhängige Cloud- Computing-Plattformen zusammenarbeiten zu lassen, ohne dass gesonderte Absprachen zwischen den Plattformen notwendig sind

- Um die Interoperabilität zu gewährleisten, müssen Anbieter von Cloud-Computing-Diensten **standardisierte oder offen gelegte Schnittstellen (API, Protokolle)** verwenden

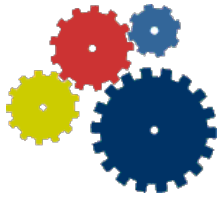
13. Datenschutz/Compliance



- Wenn in der Cloud personenbezogene Daten verarbeitet oder gespeichert werden, **muss der Schutz personenbezogener Daten gemäß den Bestimmungen des BDSG** gewährleistet sein

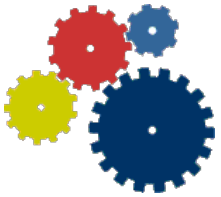
- Zudem sind vom Cloud-Anbieter die vom Cloud-Nutzer geforderten sonstigen rechtlichen Bestimmungen einzuhalten (compliance). Der Cloud-Anbieter muss hier die technischen Voraussetzungen geschaffen haben.

14. Cloud-Zertifizierung



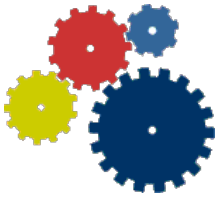
- Der Cloud-Anbieter soll sein **Sicherheitsniveau nachweisen** können. Sobald anerkannte Zertifizierungen für Cloud-Anbieter verfügbar sind, sollten diese nachgewiesen werden.
  - „Nachweis“ der Einhaltung von cloud-spezifischen Standards und Mindestanforderungen (vorliegende Mindestanforderungen des BSI), sobald solche etabliert sind (Selbstaussage)
  - Nachweis ausreichender Informationssicherheit (Zertifizierung)

15. Zusatzforderungen an Public-Cloud-Anbieter für die Bundesverwaltung



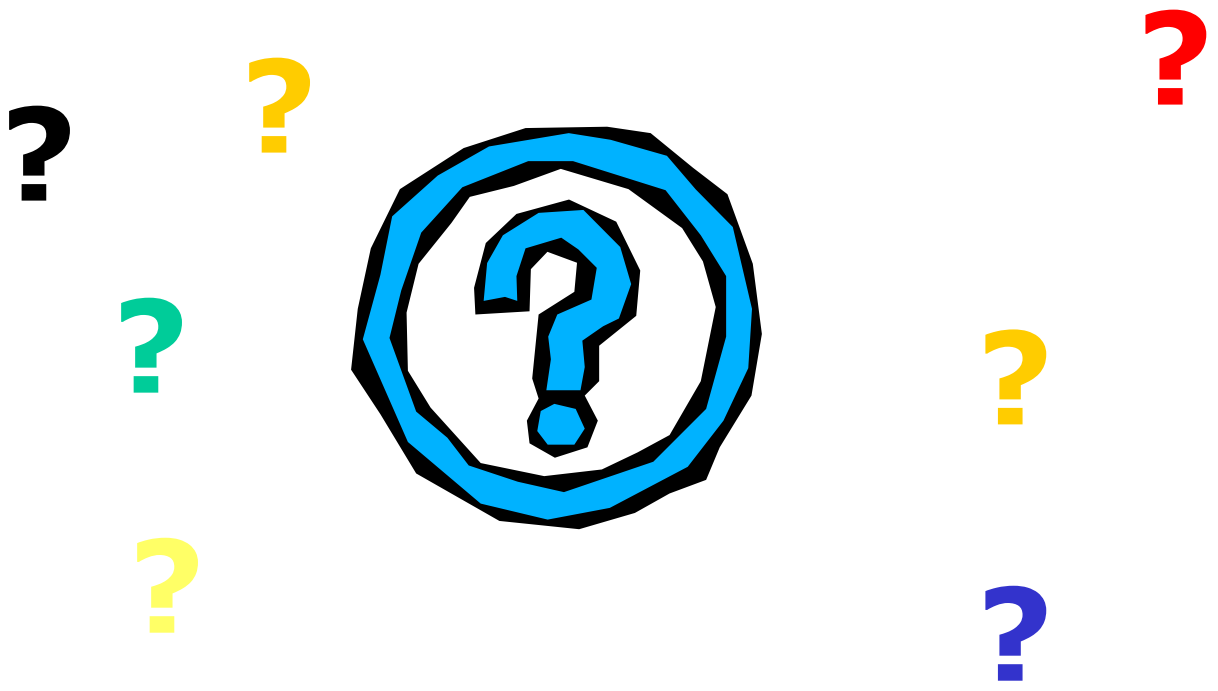
- Nutzt die Bundesverwaltung einen Cloud-Anbieter, so muss dieser weitere Forderung erfüllen.
  - Vertrag mit Gerichtsstandort Deutschland und deutsches Recht
  - IS-Revisionsrecht für das BSI stellvertretend für die Bundesverwaltung
  - Zusammenarbeit mit dem BSI-CERT und dem IT-Krisenreaktionszentrum im BSI
  - Berechtigung des BSI zur Durchführung von Penetrationstests in der Cloud

Einschränkungen



- Sollen Informationen/Prozesse mit einer **sehr hohen Vertraulichkeit** (z. B. VS-eingestufte Daten) und/oder einer **sehr hohen Verfügbarkeit** (z. B. kritische Geschäftsprozesse, IT-Anwendungen in Kritischen Infrastrukturen) in einer Public Cloud verarbeitet bzw. ausgeführt werden, so hat der Dateneigner kritisch abzuwägen, ob er die Nutzung einer Public Cloud für diese hochschutzbedürftigen Daten/Prozesse verantworten kann

Fragen und Diskussion



Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Alex Didier Essoh
Godesberger Allee 185-189
53175 Bonn
Tel: 0228-99-9582-5391

IT-Grundschutz-Hotline
Telefon: 0228-99-9582-5369
E-Mail: grundschutz@bsi.bund.de

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Clemens Doubrava
Godesberger Allee 185-189
53175 Bonn
Tel: 0228-99-9582-5887

IT-Grundschutz-Hotline
Telefon: 0228-99-9582-5369
E-Mail: grundschutz@bsi.bund.de