Stand 31.08.2012

Risikoanalyse Cloud-Computing Schweizer Behörden

Projektname: GovCloud
Projektnummer:
Version: 1.0

Beteiligter Personenkreis	
Autor:	Jonas Dischl
Bearbeitung:	Willy Müller
Prüfung:	Rolf Oppliger

Inhalt

1 Einleitung

Die Vorteile von Cloud-Computing sind unbestritten. Cloud-Computing-Angebote werden von den Behörden bereits genutzt, ob dies strategisch vorgesehen ist oder nicht [1]. Die Analysten sind sich einig, dass die Nutzung Cloud-Computing-basierter Infrastrukturen und Dienste in Zukunft stark zunehmen wird. Damit verbunden sind ernstzunehmende Risiken, die sich von bisherigen Outsourcing-Lösungen indes nicht grundsätzlich unterscheiden. Eine geeignete Strategie adressiert diese Risiken und unterstützt damit eine risikobewusste und verantwortungsvolle Nutzung von Cloud-Computing-Diensten.

Die Risiken beim Einsatz von Cloud-Computing wurden in diversen Studien im Detail untersucht. Grundlage der vorliegenden Risikoanalyse bildet insbesondere die Studie „Cloud-Computing – Benefits, Risks and Recommendations for Information Security“ der ENISA. Ergänzend wurden weitere Publikationen und eine Analyse, welche in der Strategieerabeitung von einem Expertenteam durchgeführt wurde, berücksichtigt. Damit wird auch die Besonderheiten der Situation in der Schweiz Rechnung getragen.

Das vorliegende Dokument kann die umfangreichen existierenden Studien nicht ersetzen. Es fasst die wichtigsten Risiken zusammen und beschreibt, wie sie in der Cloud-Computing-Strategie adressiert werden. Zudem wird bewertet, wie die Risiken einzuschätzen sind, wenn keine Cloud-Computing-Strategie vorgegeben wird. Eine kommentierte Liste der einbezogenen Publikationen findet sich im Anhang. Auf Grund der vorliegenden Risikoanalyse wurden einige Aussagen der Strategie präzisiert und bei den Stossrichtung die Sensibilisierung der Behörden für die Risiken des Cloud-Einsatzes aufgenommen.

2 Management Summary

Der Einsatz von Cloud-Diensten ist – wie alle Outsourcing-Lösungen – mit organisatorischen, rechtlichen und technischen Risiken verbunden. Dadurch dass Cloud-Dienste typischerweise ohne grossen Aufwand von „jedermann“ direkt über das Internet genutzt werden können, werden diese Risiken noch erhöht.

Organisatorische Risiken: Cloud-Dienste werden üblicherweise von externen Anbietern bezogen (Outsourcing), die vielfach im Ausland lokalisiert sind, und über die man typischerweise geringe Kontrolle hat.Politische Risiken (z.B. Erpressbarkeit durch Daten in ausländischer Verfügungsgewalt) werden unter rechtlichen Risiken subsumiert.

Rechtliche Risiken: Ausländische Anbieter sind in aller Regel ausländischem Recht unterstellt, das mit Schweizer Recht unter Umständen kollidieren kann. Verträge können Elemente enthalten, die das Risiko für den Service-Nutzer auf inakzeptable Weise erhöhen.

Technische Risiken: Technische Eigenheiten des Cloud-Computing eröffnen zusätzliche Angriffspunkte für Missbrauch oder böswillige Attacken.

Eine Gegenüberstellung der Risiken und der Grundsätze und Massnahmen der Cloud-Strategie zeigt, dass die Cloud-Strategie die wesentlichen Risiken, soweit dies auf strategischer Ebene möglich ist, adressiert: Für kritische Daten und Anwendungen sollen Cloud-

Infrastrukturen bereitgestellt werden, die von den Schweizer Behörden kontrolliert werden (und damit auch Schweizer Recht unterliegen). Für hochsensible Daten und Anwendungen kommen – alternativ zu bestehenden IT-Umgebungen – Behörden-eigene Private Cloud-Lösungen in Frage. Für öffentliche (und damit unkritische) Daten und Anwendungen bietet sich hingegen die Nutzung von Public Cloud-Lösungen an.

Riskant ist der Einsatz von öffentlichen Cloud-Computing-Lösungen vor allem dann, wenn er ohne vorgängige sorgfältige Evaluation und Abwägung der Risiken erfolgt. Die Strategie sieht vor, dass die Entscheidungsträger bezüglich der Gefahren des Cloud-Einsatzes sensibilisiert werden. Einfach zu nutzende Wegleitungen, Hilfsmittel und Vertragsvorlagen sowie anerkannte Standards, Zertifizierungen oder Labels sollen ihnen die verantwortungsbewusste Wahl und Nutzung von Cloud-Angeboten erleichtern.

Wird auf die Cloud-Computing-Strategie und die Umsetzung der darin formulierten Massnahmen verzichtet, ist damit zu rechnen, dass das bisherige Sicherheitsniveau der IT der Schweizer Behörden aufgrund des ungeregelten zunehmenden Einsatzes von Cloud-Diensten sinkt.

3 Beispiele der Cloud-Nutzung

Bereits heute werden Cloud-Anwendungen von den Behörden und ihren Mitarbeitern benutzt:

- **Beispiel 1: Doodle.** Doodle hilft Personen, miteinander Termine abzumachen oder Abstimmungen durchzuführen. Einzige Bedingung ist der Zugang zum Internet. Das einfach zu benutzende Werkzeug ist gerade bei Behördenmitarbeitern sehr beliebt. Wer erkundigt sich vorher, wie Doodle seine Informationen schützt?
- **Beispiel 2: Dropbox.** Dropbox stellt Speicherplatz im Internet zur Verfügung. Ein immer grösserer Personenkreis nutzt den Dienst, um mit seiner Hilfe auch grössere Datenmengen auszutauschen. Besonders in Arbeitsgruppen, Schul- und Universitätskreisen erfreut sich der Dienst immer grösserer Beliebtheit, und das, obwohl in den Medien wiederholt über Sicherheitslücken von Dropbox berichtet wurde. Das BIT sperrt daher den Zugang, behindert dadurch allerdings den Datenaustausch von Bundesmitarbeitern mit anderen Behördenstellen, die eine andere Policy fahren.
- **Beispiel 3: Microsoft Rahmenvertrag der SIK mit Office 365.** Im neuen Rahmenvertrag der SIK bietet Microsoft ihre Office Suite sowohl in klassischer Form wie auch zu attraktiven Konditionen als Cloud-Angebot Office 365 an.
- **Beispiel 4: Amazon Web Services.** Amazon bietet, wie Microsoft und andere Mitbewerber, Rechner- und Speicherleistung hoch flexibel und zu äusserst attraktiven Konditionen als Service aus der Steckdose an. Das Bundesamt für Landestopographie benutzt den Dienst für die Publikation seiner beliebten Kartendienste geo.admin.ch. Der Betrieb auf der bundesinternen Informatikinfrastruktur wäre nicht zu bezahlen und könnte den Flexibilitätsanforderungen des Dienstes nicht gerecht werden.
- **Beispiel 5: Cloud-Entwicklungsplattform des BIT.** Das BIT bietet neuerdings eine Entwicklungsplattform für Eigenentwicklungen als Cloud-Dienst an. Es konnte damit die Bereitstellungszeit um ca. das Zwanzigfache reduzieren. Ausserdem kann es auf diese Weise Entwicklungsvorgaben einfach durchsetzen, so dass sich die darauf entwickelten Anwendungen problemloser in ihre Betriebsumgebung integrieren lassen.

Die aufgeführten Beispiele machen deutlich: Cloud-Lösungen haben unbestritten ihre Vorteile, weswegen auch die Schweizer Behörden bereits heute verbreitet Cloud-Lösungen einsetzen. Sie tun dies nicht in jedem Fall bewusst und nach gründlicher Abklärung der damit verbundenen Risiken. Wenn die Schweizer Behörden sich nicht auf eine gemeinsame Strategie bezüglich der Nutzung von Cloud-Angeboten einigen, wird darunter die Zusammenarbeit zwischen den Behörden leiden. Sich widersprechende Vorgaben werden zur Folge haben, dass Konflikte auf Grund von inkompatiblen Vorgaben im Einzelfall aufwändig bereinigt werden müssen.

4 Zum Verständnis der Risikoanalyse

Zum besseren Verständnis der Risikoanalyse sind folgende Punkte zu beachten[1]:

- Cloud-Computing ist nicht gleich Cloud-Computing. Es gibt eine zunehmende Zahl von verschiedenen Ausprägungen und Anwendungen, welche unterschiedliche Risikoprofile aufweisen, jedoch im Rahmen dieses Dokuments nicht gesondert betrachtet werden können[2]. Die vorliegende Analyse beleuchtet die grundlegende Risikosituation beim Einsatz von Cloud-Computing und ersetzt keine projektspezifischen Risikoabklärungen.

- Für eine korrekte Einschätzung der Risiken von Cloud-Computing sollten diese mit den Risiken etablierter Lösungen (inkl. «klassischem» Outsourcing) verglichen werden. Dabei müssen alle Aspekte betrachtet werden. Es ist beispielsweise unzulässig, nur den Datenspeicherort (vor Ort bzw. in der Cloud) zu betrachten. Dokumente, die vor Ort gespeichert sind, werden oft unkontrolliert per E-Mail verteilt, während Cloud-Dienste unter Umständen Kollaboration und Kommunikation auf einer klar definierten Plattform erlauben. Per E-Mail können vermeintlich sicher vor Ort gehaltene Daten auf weltweit nicht kontrollierbare Server und Netzwerke gelangen. Dieser Umstand wird in der Risikoabwägung oft vergessen.

- Mit entsprechenden vertraglichen Regelungen zwischen Anbietern und Nutzern von Cloud-Computing können Risiken teilweise ausgeschlossen werden. Dies gilt jedoch nicht für alle Risiken. Beispielsweise können Konkurs oder massive Reputationsverluste eines Anbieters kaum kompensiert werden.

- Im vorliegenden Dokument wird aus Gründen der Übersichtlichkeit und Allgemeinverständlichkeit eine konsolidierte Sicht präsentiert. Insbesondere wird auf technische Details weitgehend verzichtet. Detaillierte Informationen sind bei Bedarf in den im Anhang aufgeführten Studien nachzulesen.

- Eine seriöse, aussagekräftige Quantifizierung der Risiken auf diesem Abstraktionsniveau ist nur beschränkt möglich, wird jedoch zur groben Orientierung in einer Übersichtsgraphik (Abbildung 1) vorgenommen.

Dafür wird die in der ENISA-Studie [1] eingeführte einfache Skala (0-2: tiefes Risiko, 3-5: mittleres Risiko, 6-8: hohes Risiko) übernommen. Die Bewertung der Risiken orientiert sich

[1] Diese Bemerkungen lehnen sich teilweise stark an die in der ENISA-Studie [1] erwähnten Punkte an, da diese auch für das vorliegende Dokument Gültigkeit haben.

[2] Selbst bedeutend umfangreichere Studien können diese Unterscheidung nur teilweise machen [z.B. 1]

ebenfalls an der Einschätzung dieser Studie, übernimmt sie aber nicht unreflektiert, sondern versucht, der Situation in der Schweiz Rechnung zu tragen.

5 Ergebnisse

Abbildung 1 liefert einen Überblick der Risikoprofile für drei verschiedene Szenarien:

- **Kein Einsatz von Cloud-Computing**
  Dieses Szenario geht davon aus, dass keine Cloud-Computing-Dienste eingesetzt werden. Der Fokus liegt auf der „traditionellen Leistungserbringung vor Ort“ in Kombination mit etablierten Formen des Outsourcing. Aktuelle Studien sind sich einig, dass der zunehmende Einsatz von Cloud-Computing nicht aufzuhalten ist. Dieses Szenario ist dementsprechend mittel- und langfristig unrealistisch und eher als Referenzprofil zu betrachten.

- **Strategischer Einsatz von Cloud-Computing**
  Dieses Szenario geht davon aus, dass eine Cloud-Computing-Strategie vorhanden ist und umgesetzt wird. Die Strategie regelt den Einsatz von Cloud-Computing nicht strikt, sondern definiert Grundsätze und flankierende Massnahmen, um den optimalen Cloud-Computing-Einsatz unter Verminderung der damit verbundenen Risiken zu erleichtern.

- **„Wilder“ Einsatz von Cloud-Computing**
  Dieses Szenario geht davon aus, dass die Behörden ohne koordinierende Cloud-Computing-Strategie und damit unabhängig voneinander Cloud-Computing-Dienste nutzen.

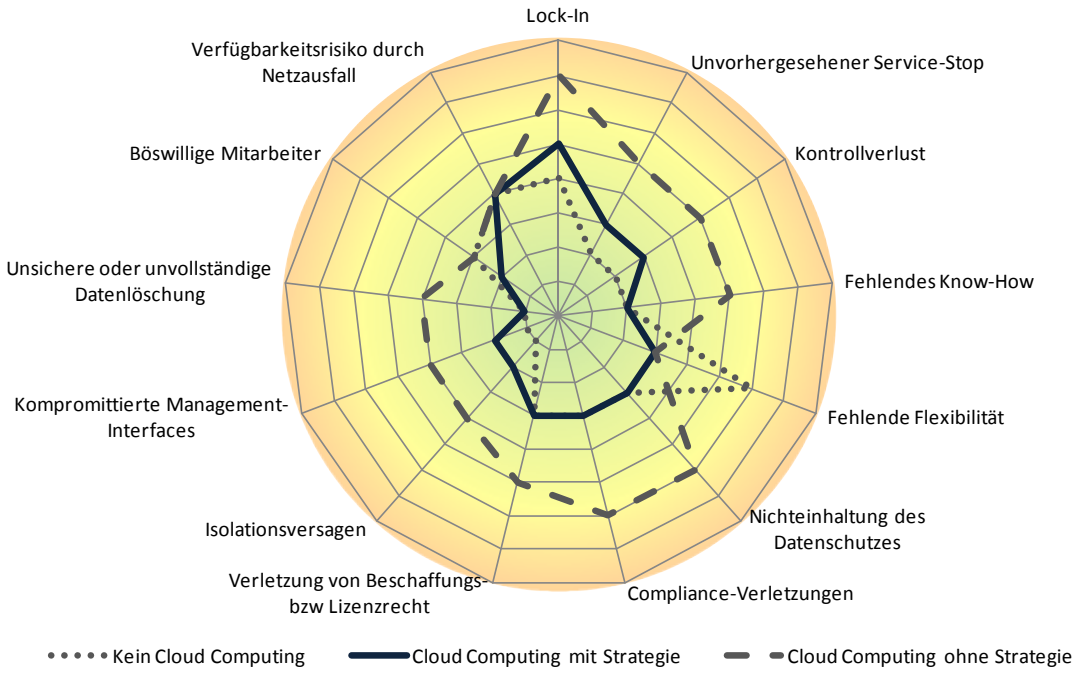

Abbildung 1: Risikoprofile im Überblick

Die meisten Risiken, welche in den verschiedenen internationalen Studien erwähnt werden, sind auch im Kontext der Schweizer Behörden relevant. Es gibt jedoch einige Aspekte, die für eine Risikoanalyse in der Schweiz besonders beachtet werden müssen.

Insbesondere die rechtlichen Rahmenbedingungen unterscheiden sich von denjenigen in anderen Ländern und bringen eigene Herausforderungen und Risiken mit sich. Da zu diesem Thema im Begleitdokument zur Cloud-Computing-Strategie umfassende Informationen vorliegen, werden sie an dieser Stelle nicht weiter ausgeführt.

Ein zentraler Bestandteil der Cloud-Computing-Strategie bildet die Bereitstellung einer von den Behörden kontrollierten Government Community Cloud, die idealerweise von Verwaltungseinheiten aller föderalen Ebenen gemeinsam genutzt werden kann (z.B. um standardisierte Dienste und Skaleneffekte zu nutzen, für die einzelne Private Cloud-Lösungen zu klein wären. Eine solche landeseigene Community Cloud reduziert die meisten Risiken. Eine gemeinsame Nutzung von Diensten setzt allerdings voraus, dass die Leistungsbezüger ihre Anforderungen bis zu einem gewissen Grad konsolidieren. Dies ist angesichts der föderalistischen Strukturen eine Herausforderung.

Cloud-Computing kann lokal die Sicherheit erhöhen

Manche Schweizer Gemeinden beziehen ihre IKT-Leistungen bei Klein- und Kleinstanbietern. Gerade in diesen Fällen würde der Wechsel hin zu geeigneten Cloud- Anbietern die Sicherheit in der Regel deutlich erhöhen. Die Konzentration von Ressourcen, Daten und professionellem Betrieb beim Cloud-Anbieter führt dazu, dass sich eine Cloud-Lösung gegenüber bisherigen aufwändigen Lösungen rechnet (z.B. physische Sicherungsmassnahmen, Einsatz von Sicherheits- und Supportspezialisten usw.). Gleichwertige Massnahmen können bei einer Leistungserbringung vor Ort aus Kostengründen oft nicht umgesetzt werden. Zudem ist das rasche Einspielen von Sicherheitsupdates in Cloud-Umgebungen einfacher und zuverlässiger realisierbar.

6 Organisatorische Risiken

Abhängigkeit vom Anbieter
Man ist an den gewählten Anbieter («Vendor Lock-in») gebunden, da ein Anbieterwechsel zu anspruchsvoll und kostspielig ist. Der Anbieter kann diese Abhängigkeit zu seinem eigenen einseitigen Vorteil ausnutzen.

Unvorhergesehener Service-Stop
Die bezogenen Services sind im schlimmsten Fall ohne Vorwarnung nicht mehr oder nur noch unter stark veränderten Bedingungen verfügbar.

Kontrollverlust
Da Infrastruktur, Applikationen und Daten beim Anbieter sind, kann die Einhaltung von Sicherheitsvorgaben nur schwer vorgegeben und kontrolliert werden. Eigene Anforderungen können nur bedingt durchgesetzt werden.

Anbieterunabhängige Standards und Werkzeuge fördern die Interoperabilität und Portabilität von Daten und Anwendungen zwischen Cloud-Anbietern und vereinfachen die Migration. Sie erleichtern damit den Anbieterwechsel und vermindern die Abhängigkeit von einem spezifischen Anbieter. Standardisierungsaktivitäten sind im Gange (z.B. OCI), jedoch noch nicht weit fortgeschritten.

Unvorhersehbare Ereignisse wie z.B. der Konkurs oder Aufkauf eines Anbieters oder Subunternehmers können dazu führen, dass Daten oder Dienstenicht mehr zur Verfügung stehen. Wie gross dieses Risiko ist, hängt stark von der Wahl geeigneter und vertrauenswürdiger Anbieter und Services ab.

Zumindest teilweise gibt der Cloud-Nutzer die direkte Kontrolle über den Umgang mit seinen Daten und Applikationen wie auch über die Umsetzung der Sicherheits- und Compliancevorgaben aus den Händen. Zusicherungen müssen soweit möglich vertraglich geklärt werden. Eine weitere Möglichkeit bilden Audits oder eine Zertifizierung bzw. ein Labeling von Angeboten.

Durch geeignete Unterstützung in der Angebotswahl können die Risiken einer Abhängigkeit von Dritten verkleinert werden. Sie werden jedoch von der ENISA-Studie als leicht höher als in der traditionellen Leistungserbringung eingeschätzt.

Strategie:

- Die Cloud-Strategie sieht vor, dass für kritische Daten und Anwendungen von den Behörden kontrollierte Community Cloud-Dienste bereitgestellt werden, damit in diesem Bereich die negativen Auswirkungen der Abhängigkeit von einem externen (evtl. ausländischen) Provider minimiert werden können (Stossrichtung S3).
- Die Behörden sollen auf nationaler und internationaler Ebene die Bereitstellung von Cloud-Standards fördern und diese von den Cloud-Anbietern fordern (Grundsatz G7).
- Es sollen Wegleitungen und Vertragsvorlagen erstellt werden, welche die sorgfältige Anbieterauswahl und den Vertragsabschluss unterstützen.
- In einer Studie soll abgeklärt werden, inwiefern Zertifizierungen oder Labels (Stossrichtung S1) zur Risikominderung beitragen können.

Fehlendes Know-How
Fehlendes Know-How und fehlende Erfahrungen im Umgang mit Cloud-Computing können dazu führen, dass ungeeignete Anbieter gewählt, problematische Verträge abgeschlossen, Lösungen mit Sicherheitslücken implementiert, mit den Daten leichtfertig umgegangen und absichernde Begleitmassnahmen vernachlässigt werden.

Der verantwortungsbewusste Einsatz von Cloud-Diensten verlangt entsprechende Kenntnisse, sowohl auf Seiten der Leistungsbezüger (z.B. Kenntnis der Risiken, Angebotsevaluation, Integration) wie bei den Cloud Service-Anbietern. Dieses Wissen ist noch nicht weit verbreitet. Da Cloud-Computing relativ neu ist und sich noch immer rasch entwickelt, fehlen zudem systematische Langzeiterfahrungen.

Strategie:

Die Strategie sieht vor, dass der Einsatz von Cloud-Diensten in den Behörden schrittweise, nicht auf einen Schlag erfolgt. Die Erfahrungen – positive wie negative – sollen kommuniziert werden, damit alle daraus lernen können. Parallel dazu ist das notwendige Know-how bei Leistungsbezügern und Leistungserbringern zu verbessern (Stossrichtung S1).

Fehlende Flexibilität
Die IKT kann die Geschäftsanforderungen nicht in nützlicher Frist umsetzen: • Kurzfristige Belastungsspitzen können nicht abgefangen werden und führen zu Einschränkung oder Ausfall eines Dienstes. • Nicht mehr benötigte Ressourcen (Hardware, Lizenzen…) verursachen weiterhin Kosten. • Die Bereitstellung von dringend benötigten Diensten ist nicht zeitgerecht möglich.

Viele Organisationen sind mit einem zunehmend dynamischen Umfeld konfrontiert. Ein sich rasch veränderndes Umfeld kann die zeitnahe Bereitstellung von neuen Diensten notwendig machen.

Cloud-Computing bietet im Vergleich zur klassischen Leistungserbringung vor Ort typischerweise höhere Flexibilität bei der Bereitstellung der benötigtenRessourcen. Zusätzliche Ressourcen können rasch zugeschaltet, nicht mehr benötigte wieder freigegeben werden. Die Ressourcen (Infrastrukturen, Anwendungen) sind für alle auf dem neusten Stand. Da keine aufwändigen Realisierungsprojekte benötigt werden, können Dienste rasch in Betrieb genommen werden.

Strategie:

Behörden sollen zur Erhöhung ihrer Flexibilität Cloud-Dienste einsetzen, sofern damit nicht andere relevante Sicherheitsanforderungen (Vision, Grundsatz G2) verletzt werden.

7 Rechtliche Risiken

Nichteinhaltung der rechtlichen Vorgaben und ungeeignete Verträge
Cloud-Dienste werden über das Internet angeboten. Der Anbieter kann im Ausland domiziliert sein oder die Daten eventuell in Rechenzentren in unterschiedlichen Ländern speichern. Dabei kommen jeweils andere lokale Gesetzgebungen zum Zuge. Diese müssen nicht in jedem Fall mit jenen der Schweiz kompatibel sein. Sanktionen und Reputationsschäden auf Grund von Verletzungen der rechtlichen Vorgaben können die Folge sein.

Beim Einsatz von Cloud-Computing-Diensten besonders kritisch zu betrachten sind:
- Datenschutzgesetz und nationale Gesetze zur Weitergabe von Daten, z.B. an den Staat
- Fernmeldegesetz und andere branchenspezifische Bestimmungen
- Beschaffungs-, Vertrags- und Lizenzrecht
- kantonale Gesetzgebungen und Regelungen (beispielsweise bezüglich des Ortes der Leistungserbringung)

Das aktuelle Beschaffungsrecht von Bund und Kantonen ist nicht auf die Besonderheiten der Leistungserbringung im Cloud-Computing ausgelegt. Zudem können sich lizenzrechtliche Probleme ergeben, wenn beispielsweise eine bisher lokal genutzte Software auf einer Umgebung in der Cloud installiert wird.[3]

[3] Aufgrund der Besonderheiten von Cloud-Computing wurde bei der Erarbeitung der Strategie der Behörden ein besonderes Augenmerk auf die rechtlichen Rahmenbedingungen gelegt. Im Kommentar zur Strategie finden sich hierzu detaillierte Informationen.

Strategie:

Die rechtlichen Risiken sind bei der Evaluation eines Cloud-Dienstes zu analysieren und bei der Formulierung der Bezugsverträge zu berücksichtigen. Die Strategie sieht vor, dass den Behörden Wegleitungen und Vertragsvorlagen zur Verfügung gestellt werden, welche diese Risiken minimieren helfen (Stossrichtung S1). Bund und Kantone sind aufgefordert, ihre Gesetzgebungen daraufhin zu überprüfen, ob sie den Einsatz von Cloud-Diensten durch die Behörden adäquat abdecken. Wenn das nicht der Fall ist, sind die vorhandenen Vorgaben anzupassen (Stossrichtung 2).

8 Technische Risiken

Technische Risiken können insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit von Daten oder Applikationen gefährden. Zentrale Risiken sind:

Isolationsversagen
Im Cloud-Computing teilen sich verschiedene Anwender oft dieselben (physischen) Ressourcen. Die Mechanismen, welche für eine saubere Trennung der Daten verschiedener Anwender sorgen, können ausfallen, so dass Cloud-Dienst-Nutzer auf Daten anderer Cloud-Dienst-Nutzer Zugriff bekommen.

Kompromittierte Management-Interfaces
Viele Cloud-Computing-Angebote können über das Internet genutzt und verwaltet werden. Damit existiert im Vergleich zu anderen Leistungserbringungsarten ein zusätzlicher Angriffspunkt, über den Unbefugte sich Zugang zu Anwendungen und Daten verschaffen können.

Unsichere oder unvollständige Datenlöschung
Werden Daten nicht wie vom Kunden verlangt vollständig gelöscht – beispielsweise weil der Anbieter dazu nicht in der Lage ist – erhöht sich das Risiko, dass diese in falsche Hände geraten.

Böswillige Mitarbeiter
Cloud-Computing-Architekturen erfordern zur Pflege Rollen mit hohen Privilegien. Ein böswilliger Mitarbeiter hat unter Umständen die Möglichkeit, Manipulationen an Daten vorzunehmen, diese an Unbefugte weiterzugeben oder die Verfügbarkeit eines Dienstes zu stören.

Fehlende Verfügbarkeit
Cloud-Computing-Dienste werden über Netzwerke bezogen und genutzt. Ungenügende Bandbreite kann dazu führen, dass die Dienste nicht mehr nutzbringend eingesetzt werden können. Bei einem Netzausfall sind sie nicht mehr verfügbar.

Strategie:

Die konkreten Risiken müssen projektspezifisch analysiert und adressiert werden. Dies kann eine Risikoanalyse auf strategischer Ebene nicht leisten. Die Strategie hält folgerichtig fest, dass der Cloud-Nutzer selbst die Verantwortung für seine Daten und Anwendungen trägt (Grundsatz G3). Er muss projektspezifische Risikoanalysen durchführen. Dies gilt auch, aber nicht nur für die technischen Risiken. Bei der Evaluation und beim Einsatz von Cloud-Computing-Diensten ist Sicherheitsaspekten gebührend Rechnung zu tragen (Grundsatz G9). Um dies zu erleichtern, sollen Hilfsmittel, insbesondere auch zur Beurteilung der Sicherheitsrisiken bereitgestellt werden (Stossrichtung S1).

9 Auswirkungen des Verzichts auf eine Strategie

Cloud-Dienste können typischerweise und ohne viel Umstände von „jedermann“ direkt über das Internet beschafft und genutzt werden. Im Vergleich zu anderen Leistungserbringungsarten erhöht diese Tatsache die Gefahr einer schnellen Nutzung ohne sorgfältige vorgängige Evaluation entscheidend. Ohne eine mit geeigneten Massnahmen lenkende und informierende Strategie ist das Risiko, dass beispielsweise aus Kostengründen oder aus mangelndem Know-how unzureichend geprüfte Cloud-Angebote genutzt werden, hoch, zumal vor allem kleinere Einheiten kaum Ressourcen für eine sorgfältige Evaluation haben.

Werden zudem statt einer gemeinsamen Cloud-Computing-Strategie der Behörden lokale, nicht aufeinander abgestimmte Strategien definiert, kann dies zu Problemen in der Zusammenarbeit (Interoperabilität von Prozessen und Services) unter den Behörden führen, wodurch wirtschaftliche Vorteile des Cloud-Computing nicht genutzt werden können und das Risiko von Sicherheitslücken durch schlecht aufeinander abgestimmte Services steigt.

Wird auf die Cloud-Computing-Strategie und die Umsetzung der darin formulierten Massnahmen verzichtet, ist damit zu rechnen, dass das durchschnittliche Sicherheitsniveau der IT der Schweizer Behörden auf Grund des unkontrolliert zunehmenden Einsatzes von Cloud-Diensten sinken wird.

A. Liste der berücksichtigten Studien

Im Folgenden sind die wichtigsten Publikationen aufgeführt, welche für die vorliegende konsolidierte Sicht berücksichtigt wurden.

Es wird empfohlen, für projektspezifische Risikoanalysen auf diese Studien zurückzugreifen.

[1]	Cloud-Computing Benefits, Risks and recommendations for information security (ENISA, November 2009)	Eine ausführliche Auflistung von Sicherheitsvorteilen und Risiken der Cloud inklusive Empfehlungen und einer umfassenden Checkliste.
[2]	Security & Resilience in Governmental Clouds (ENISA, Januar 2011)	Untersucht Sicherheitsaspekte mit Fokus auf Governmental Clouds und bietet entsprechende Hilfestellungen.
[3]	Leitfaden Cloud-Computing Risk&Compliance Schweiz (EuroCloudSwiss, März 2012)	Eine Studie, welche die Situation in der Schweiz berücksichtigt und den Fokus auf Compliance und Vertragsgestaltung setzt.
[4]	Cloud-Computing für die öffentliche Verwaltung (ISPRAT-Studie November 2010)	Diese Studie hat das Ziel, die Potentiale von Cloud-Computing für den deutschen öffentlichen Sektor aufzuzeigen und kritisch zu beleuchten.
[5]	Cloud-Computing Sicherheit Schutzziele, Taxonomie, Marktübersicht (Fraunhofer AISEC, Sept 2009)	Eine Studie zum Thema Cloud-Computing-Sicherheit mit Stand September 2009 inklusive einer Taxonomie von Sicherheitsaspekten.
[6]	Security Guidance for critical Areas of focus in Cloud-Computing V3.0 (CSA, 2011)	Eine ausführlicher Zusammenstellung von Sicherheitsrichtlinien unter Einbezug von 70 internationalen Experten.
[7]	Top Threats to Cloud-Computing V1.0 (Cloud Security Alliance, 03/01/2010)	Eine kurze Auflistung zentraler Risiken in Ergänzung zum ausführlichen Richtliniendokument der CSA [6]
[8]	Guidelines on Security and Privacy in Public Cloud-Computing (National Institute of Standards and Technology. US Department of Commerce, December 2011)	Untersuchung der Sicherheits- und Datenschutzrisiken von Public Cloud-Computing des amerikanischen NIST.