

Sicherheit im Cloud Computing – Metriken und Reporting

Cloud Computing ist ganz gewiss keine Revolution in der Informationstechnologie. Es verspricht jedoch den auslagernden Unternehmen einen wahren Goldsegen, denn das IT-Outsourcing sollte dabei nicht nur neu – nutzer- und bedarfsgerechter - organisiert, sondern auch preiswerter werden. Durch die Synergien, welche im Rahmen von Grössendegression bei der Nutzung (und / oder Stilllegung) von IT-Kapazitäten realisiert werden können, wird ein hohes Einsparpotenzial im Bereich der IT erwartet. Der Begriff der „economies of scale“ erlebt durch das Cloud Computing erneut seine Renaissance.



Dr. Aleksandra Sowa

Tätig bei der Deutschen Telekom AG. Leitete u.a. das Horst Görtz Institut für Informationstechnik und war als IT-Revisor in der Finanzdienstleistungsbranche tätig.

Software as a Service (SaaS) ist ein Beispiel dafür, wie die Kosten für Reduktion oder gar Verzicht auf die Wartung der Systeme, interne Ressourcen und Infrastruktur durch Auslagerung in eine Cloud gespart werden können. Das Versprechen der Auslagerung in eine Cloud ist, dass das Unternehmen nur dafür zu zahlen braucht, was es auch tatsächlich braucht und nutzt. Weit gefehlt – stellt ServiceNow in einem aktuellen White Paper fest – insbesondere wenn es um IT Service Management geht. Denn nicht gründlich durchdachte oder voreilige Entscheidungen über Auslagerung der IT, um schnelle Savings zu realisieren, können verheerende Konsequenzen haben. „Tally up spending on customization, piece-part licensing and upgrades, and the cost of ownership can reach obscene proportions – an extra quarter of a million dollars here, a half a million there“ – warnen die Autoren (ServiceNow 2011).

In fünf Schritten zu einer Cloud

Eine Auslagerung von IT-Dienstleistungen in eine Cloud erfordert systematischer Vorbereitung, strukturierter Verfah-

ren und Prozesse sowie viel Disziplin bei der Umsetzung geplanter Vorgehensweisen. Zuerst sollen laut Richter (2011) die Anforderungen an Kontrollen, Monitoring und Reporting sowie den Prozess der Risikobewertung für die auszulagernde IT-Systeme und -Prozesse dokumentiert werden.

security-zone 2011

Alles zum Thema Security-Monitoring

Mehr dazu im Referat von Dr. Aleksandra Sowa am Montag 10. Oktober um 14.00 Uhr.

Details & Anmeldung [hier](#)

Das Cloud Computing ist eine neuartige Form des IT-Outsourcing (Bitkom 2009) und stellt im Hinblick auf die regulatorische Anforderungen, wirksame Kontrollen in der IT (wie auch durch die IT) einzurichten und die Wirksamkeit dieser nachweisen zu können, eine neue Herausforderung für die Unternehmen dar. Denn gleich, ob Dienstleistungen externer Anbieter in Anspruch genom-

men, Fremdprogramme oder Eigenentwicklungen eingesetzt werden: den Unternehmen obliegt es, die Wirksamkeit der Kontrollen nachweisen zu können (spätestens im Rahmen einer Abschlussprüfung).

Das auslagernde Unternehmen muss im Vorfeld der Entscheidung über die Nutzung von Cloud auf Grundlage einer Risikoanalyse eigenverantwortlich festlegen, welche Aktivitäten und Prozesse überhaupt ausgegliedert werden dürfen (vgl. MaRisk VA). Und dies zu dokumentieren. Bei besonders schweren bzw. kritischen Risiken werden die Aktivitäten und Prozesse erst gar nicht ausgelagert bzw. die Auslagerung ist ggf. zu beenden.

Dementsprechend ist auch das Anforderungsmanagement anzupassen sowie die an der Vertragsgestaltung beteiligten Mitarbeiter, insbesondere die für Vertragsabschlüsse verantwortlichen Juristen, zu sensibilisieren und auszubilden, damit die Besonderheiten des IT-Outsourcing in die Cloud in den Verträgen hinreichende Berücksichtigung finden. Insbesondere auch diese Anforderungen, welche sich auf das Monitoring und Reporting beziehen, sind zu beachten.

Monitoring und Reporting sind essentiell, wenn es um die Bewertung und Beurteilung der Effektivität der Kontrollen bei der Auslagerung der IT geht. Das Reporting ist vor dem produktiven Einsatz zu testen, damit der Nachweis seiner Effektivität erbracht werden kann. Das Reporting ist nicht nur zur Bewertung der regulatorischen Compliance, Effizienz oder Effektivität der Kontrollen relevant. Ebenfalls ist die Kommunikation der

der kumulierten, relevanten Ergebnisse an das Management sinnvoll, um Transparenz im auslagernden Unternehmen zu schaffen und dem Management zuverlässige Grundlagen für ihre Entscheidungen (u.a. bzgl. weiterer Auslagerungen) vorzulegen.

Überwachung der Informationssicherheit in der Cloud

Zwei Aspekte der IT-Kontrollen und Informationssicherheit kommen beim Cloud Computing besonders zur Geltung. Erstens, müssen die Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit von Informationen für jede Art von Auslagerung (SaaS, PaaS oder IaaS) gewährleistet werden. Dies bedeutet, dass die relevanten Kontrollen von dem auslagernden Unternehmen definiert, von dem Cloud-Anbieter nachweislich implementiert sowie ihre Effektivität im Rahmen des Monitoring überwacht und im Reporting an den Cloud-Nutzer berichtet wird. Zweitens, können Teile des Informationsmanagements bzw. generelle Kontrollen wie Identitätsmanagement, Zugriffsmanagement etc., gänzlich ausgelagert werden. Die letztere Dienstleistung fungiert oft unter dem Namen Security Software as a Service (Security SaaS) und wird inzwischen von zahlreichen Anbietern (Symantec, Microsoft und McAfee gehören zu den am öftesten von den US-Cloud-Nutzern genannten Neman) angeworben. Zu den aktuell am meisten in den Unternehmen verbreiteten Typen der Security SaaS gehören Messaging bzw. E-mail Security, URL Filtering, Endpoint Antivirus und Web Application Firewall (WAF). Die

Angebote der Security SaaS, welche sich aktuell noch keiner grossen anfrage erfreuen (vgl. Studie von: Hochmuth 2011), können leicht auf weitere Bereiche der Informationssicherheit ausgeweitet werden.

Bei der Definition von Minimalanforderungen an das Sicherheitsmonitoring und Incident-Management sind die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) besonders hilfreich. Das BSI stellte eine Liste von Anforderungen zusammen, welche ein Cloud-Nutzer an den Cloud-Anbieter stellen kann, und der letztere auch erfüllen sollte, falls seine Dienstleistungen die Mindestanforderungen an die Datensicherheit und -verfügbarkeit erfüllen (BSI 2011). Zu diesen Anforderungen zählen u.a. die 24/7 Überwachung der Cloud, darunter auch Logdatenerfassung und -auswertung. Das Incident-Management des Cloud-Anbieters sollte so eingerichtet sein, dass interne Angriffe von Cloud-Nutzern auf andere Cloud-Nutzer erkannt werden. Ebenfalls soll sichergestellt werden, dass 24/7 auf Angriffe, die aus der Cloud heraus durchgeführt werden, reagiert werden kann. Die Reaktionsfähigkeit auf die etwaige Verletzungen der Grundwerte der Informationssicherheit wird gewährleistet, indem 24/7-erreichbares, handlungsfähiges Cloud-Management und Trouble-Shooting verfügbar ist. Die Verfügbarkeit der Services ist zu überwachen und zu messen, und die Messergebnisse sind den Kunden zur Verfügung gestellt werden.

Von einem Cloud-Anbieter wird ebenfalls eine Einbindung in der CERT-Strukturen und das na-

tionale IT-Krisenmanagement erwartet.

So gelten für das Cloud Computing zuerst die gleichen strengen Auflagen bezüglich Sicherheit und Schutz von Informationen, wie für jede andere Auslagerung der IT.

Reporting an das Management

Über die Erfüllung der o.g. Anforderungen die Datensicherheit und -Verfügbarkeit sowie etwaige Sicherheitsvorfälle bzw. Verstöße gegen die Grundwerte der Sicherheit berichtet der Cloud-Anbieter an das auslagernde Unternehmen im Rahmen des Reporting. Der Detaillierungsgrad von traditionellen Incident-Reports, Auswertungen von Logdaten oder Verfügbarkeitsreports ist allerdings zu hoch – und zu technisch – um diese an das Management als Zielgruppe zu richten. Zwar sind die Risiken, welche den Fortbestand des Unternehmens gefährden könnten, unmittelbar (ad hoc) an das Management zu kommunizieren. Die Kriterien hierfür sollen im Vorfeld festgelegt werden, um zu verhindern, dass das Management mit einer Wüste an ad hoc Meldungen überschüttet wird. Die Wesentlichkeitsgrenzen bzw. kritische Werte für die Kommunikation an das Management sind festzulegen. Für die Krisen- und Notfälle sind neben den Kategorien ebenfalls die Berichtswege sowie die Empfänger der Informationen (beispielweise Krisenteam) festzulegen.

Alle anderen im Zusammenhang mit der Auslagerung der IT in eine Cloud relevanten Risiken, Bewertungen und Beurteilungen können im Rahmen des Management-Reporting, also in den

Monats- oder Quartalsreports zur Lage der Sicherheit (z.B. Lageberichte an die Geschäftsführung) berichtet werden. Dabei können folgende Metriken Berücksichtigung finden, bei welchen der allgemeine Zustand der Sicherheit bei IT-Auslagerungen (unabhängig von der Art und Anzahl der Anbieter) zum Tragen kommt.

Metriken zur ordnungsmässigen Umsetzung des IT-Outsourcing;

- Anteil der Cloud-Anbieter, für welche Richtlinien, Prozeduren und Kontrollen vertraglich festgelegt wurden (in Prozent).

- Anteil der Verträge mit Cloud-Anbieter, welche eine Bestätigung / Prüfung über eine unabhängige Verifizierung der Richtlinien, Prozeduren und Kontrollen umfassen (in Prozent).

- Anteil der Cloud-Anbieter, bei welchen die Einhaltung (Compliance) von Richtlinien, Prozeduren und Kontrollen im laufenden Quartal geprüft wurde (in Prozent).

Metriken bzgl. Sicherheitsvorfälle, Zugangs- und Zugriffsberechtigungen und Notfallmanagement, anhand welcher die Wirksamkeit der implementierten Kontrollen beurteilt werden kann (Auswahl).

- Anteil der Cloud-Anbieter, bei welchen Mängeln bei der Einhaltung (Compliance) von Richtlinien, Prozeduren und Kontrollen festgestellt und diese Mängel in der aktuellen Berichtsperiode ausgeräumt wurden (in Prozent, nach Kritikalität der Mängel).

- Anteil der Sicherheitslücken, welche bei den Cloud-Anbietern oder mit Bezug auf die Beziehung zu diesen festgestellt wurden (in Prozent, nach Kritikalität und Sicherheitsdomäne).

- Anteil der Sicherheitsvorfälle (Incidents) in der Berichtsperiode und in den vergangenen 12 Monaten, welche bei den Cloud-Anbietern oder mit Bezug auf die Beziehung zu diesen festgestellt wurden (in Prozent, nach Kritikalität und Sicherheitsdomäne).

- Anteil der kritischen Assets, zu welchen kein Zugriff durch die Mitarbeiter eines Cloud-Anbieters nicht erlaubt sind (in Prozent).

- Anteil der kritischen Assets, zu welchen keine Netzverbindung zu einem Outsourcing-Partner (darunter Cloud-Anbieter) erlaubt ist (in Prozent).

- Anteil der Mitarbeiter der Outsourcing-Partner (darunter Cloud-Anbieter), bei welchen in der Berichtsperiode ihre Zugriffsrechte geprüft und validiert wurden, nach Kritikalität der Assets und Sensitivität der Daten (in Prozent).

- Anteil der Verträge mit Cloud-Anbieter, welche

- a) Konsistent mit den Datenschutz- und Sicherheitsvorgaben sind

- b) Verfügbarkeit von Informationen über Sicherheitsvorfälle (Incident-Reports) sicherstellen

- c) Zur Partizipation an Trainings zur Sicherheit, Sensibilisierungsaktivitäten und Notfallübungen sicherstellen

- d) Geldbussen und / oder andere Sanktionen bei Nichteinhaltung von Richtlinien, Prozeduren und Kontrollen verhängen.

Vorteil des Cloud Computing ist u.a., dass viele Kontrollen automatisiert und somit im Rahmen standardisierter Auswertungen auf ihre Effektivität bewertet und beurteilt werden können. Empfehlenswert – insbesondere im Hinblick auf die

Kosten der Auslagerung – ist die Inanspruchnahme standardisierter Lösungen des Cloud-Anbieters anstelle individueller Lösungen. Abhängig von der nationalen Gesetzgebung oder im Hinblick auf verbindliche Branchenstandards sowie Vereinbarungen und Verträge, können die Metriken zur Bewertung und Beurteilung der Effektivität relevanter Kontrollen und Security Compliance in einem geregelten Verfahren leicht abgeleitet werden. Eine auf diesem Gebiet immer stärkere Bedeutung gewinnende Methode, welche die Unternehmensziele mit den IT-Indikatoren zu verknüpfen weiss, ist das sog. Goal-Question-Paradigma (mehr zur Methodik in: Sowa 2011).

Conclusion

Sobald die Kontrollen identifiziert sind und die entspr. Metriken zur Bewertung Effektivität des Security dieser festgelegt wurden, muss der Cloud-Anbieter ein wirksames Monitoring implementieren und dem Cloud-Nutzer aussagekräftige Daten bzw. Reports verfügbar machen. Monitoring und Reporting sind daher ein wesentlicher Teil der IT-Auslagerungsverträge und sollen im Vorfeld der Auslagerung in die Cloud definiert werden. Eine nachträgliche Implementierung der Kontrollen und des Monitoring dieser kann mit erheblichen Mehrkosten verbunden werden und damit die von Cloud Computing erwarteten Ersparnisse zunichte machen. Aber auch aus einem anderen Grund kann es sinnvoll sein, Vorsorge für die ordnungsmässige und wirksame Implementierung der IT-Kontrollen zu treffen. Mit

steigender Marktdurchdringung und Verbreitung des Cloud Computing werden die Ressourcen in zentralen Rechenzentren für die Angreifer attraktiver, wie das BSI im aktuellen Sicherheitsbericht warnt.

Quellen

BaFin. 2009. Rundschreiben 3/2009 (VA) - Aufsichtsrechtliche Mindestanforderungen an das Risikomanagement (MaRisk VA). http://www.bafin.de/cln_152/nn_721290/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2009/rs_0903_marisk_va.html

Bitkom. 2009. Cloud Computing – Evolution in der Technik, Revolution im Business. BITKOM-Leitfaden (Oktober 2009). http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf

BSI. 2011. BSI-Lagebericht IT-Sicherheit 2011. Bundesamt für Sicherheit in der Informationstechnik.

Hochmuth, P. 2011. "2011 Cloud Security Survey: Trends in Security for, and from, the Cloud". IDC Web Conference, 19 July 2011.

Ritter, J. 2011. Data governance: Five steps to cloud solution success. <http://searchcompliance.com/>

ServiceNow. 2011. SaaS Economics - The Safe Bet is No Longer the Smart Bet. http://docs.media.bitpipe.com/io_10x/io_100063/item_417775/WP0511-SaaS.pdf

Sowa, A. 2011. Metriken - der Schlüssel zum erfolgreichen Security und Compliance Monitoring: Design, Implementierung und Validierung in der Praxis. Vieweg+Teubner Verlag.