MUSTERLÖSUNG, H.P. KÖNIGS, SPRINGER VIEWEG „IT-RISIKOMANAGEMENT MIT SYSTEM“, 5. AUFLAGE

KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 16

Lösung zu Frage 1

Die drei im NIST Standard 800-145 beschriebenen Service-Modelle sind:

- ***Software as a Service (SaaS):*** *Dem Konsumenten werden in einer Cloud-Infrastruktur die Applikationen des Providers zur Benutzung bereitgestellt. Der Konsument kann die den Applikationen unterliegende Cloud-Infrastruktur (Netzwerke, Server, Betriebssysteme, Speicher etc.), abgesehen von begrenzten benutzer-spezifischen Konfigurationseinstellungen, weder steuern noch kontrollieren.*
- ***Platform as a Service (PaaS):*** *Dem Konsumenten werden Plattformen für seine Applikationen (selbst- oder fremdentwickelte) zur Benutzung bereitgestellt. Dabei werden durch den Provider bestimmte Programmiersprachen, Libraries, Services und Tools unterstützt. Der Konsument kann die den Applikationen unterliegende Cloud-Infrastruktur(Netzwerke, Server, Betriebssysteme, Speicher etc.) weder steuern noch bei Nutzung und Angebot von Cloud-Computing kontrollieren, hat aber die Kontrolle über seine bereitgestellten Applikationen sowie allenfalls über die Konfigurations-einstellungen der Applikations-Umgebung.*
- ***Infrastructure as a Service (IaaS):*** *Dem Konsumenten werden in einer Cloud-Infrastruktur des Providers grundlegende Computer-Ressourcen wie Prozessorkapazität, Speicher, Netzwerke usw. zur Benutzung bereitgestellt. Der Konsument kann auf dieser Infrastruktur beliebige Software mit entsprechenden Betriebssystemen und Applikationen einsetzen, wobei er die unterliegende Cloud-Infrastruktur weder steuern noch kontrollieren kann. Jedoch kontrolliert der Konsument seine bereitgestellten Betriebssysteme, Speicher und eingesetzten Applikationen sowie, in allenfalls begrenztem Umfang, bestimmte Netzwerk-Komponenten (z. B. Host Firewalls).*

Lösung zu Frage 2

Die aus Kundensicht typischen Sicherheitsprobleme, die im Rahmen des Risiko-Assessments näher untersucht werden müssen, sind:

1. **Privilegierte Zugriffsrechte:** Ein potenzieller Provider sollte Auskunft darüber geben, wie privilegierte Administratoren bei ihrer Einstellung überprüft, bei ihren Aktivitäten kontrolliert und vor allem wie ihre Zugriffe überwacht werden.
2. **Gesetzliche und regulatorische Compliance:** Cloud-Computing-Provider, die eine eingehende Überprüfung von Compliance-Anforderungen verweigern, kommen lediglich für triviale Services in Frage.
3. **Daten-Lokalisierung:** Der Provider sollte sich auf das Verarbeiten und Speichern der Daten innerhalb bestimmter Jurisdiktionen und auf die Nennung und die Beachtung der lokalen Datenschutz-Anforderungen verpflichten.

4. **Daten-Segregation:** Die Abschottung der Daten von anderen Kunden (Konsumenten) kann zwar mit Chiffrierung wirksam durchgeführt werden. Diese muss einerseits konsequent urchgeführt sein und darf andererseits die Verfügbarkeit (z. B. im Fehlerfalle) nicht beeinträchtigen. Der Provider sollte deshalb beweisen, dass die angewandten Chiffrier-Schemata funktionstüchtig entworfen und getestet sind.
5. **Recovery:** Die Frage ist zu klären, wie mit Desaster umgegangen wird, u. a. die Fähigkeit einer kompletten Restaurierung innerhalb konkreter Zeiterfordernisse.
6. **Unterstützung bei Nachforschungen:** Falls der Cloud-Computing-Provider sich nicht vertraglich verpflichten kann, die Nachforschungen mit entsprechenden Nachvollzugsmethoden (z. B. Logging) zu unterstützen und/oder keine Beweise dafür erbringen kann, muss davon ausgegangen werden, dass im Bedarfsfalle keine Nachforschungen möglich sein werden.
7. **Langfristige Überlebensfähigkeit:** Der potenzielle Provider muss die Frage beantworten, was mit den Daten im Falle einer Unternehmensaufgabe oder -fusion passiert. Ob beispielsweise in solchen Fällen die Daten vollständig in einem derartigen Format und in einer Weise ausgegeben werden, dass sie in einem alternativen Serviceangebot wieder importiert werden können.

Lösung zu Frage 3

Cloud-Computing- Angebote weisen in der Regel Schwachstellen auf, die von Anbieter zu Anbieter unterschiedlich ausgeprägt sind. Auch sind die in die Cloud auszulagernden Risikoobjekte unterschiedlich auf einzelne Bedrohungen und Schwachstellen anfällig. Viele der Schwachstellen hängen mit dem durch den Provider verfolgten Geschäftsmodell zusammen und können bei einem bestimmten Provider nicht ohne weiteres eliminiert werden (z.B. Auslagerung der Daten auf Speichmedien in Länder mit fragwürdigem Datenschutz). Da auch die Bedrohungen meist gegeben sind, hängt die Sicherheit der auszulagernden Risikoobjekte in einem hohen Ausmass von den beim Provider vorkommenden inhärenten Schwachstellen ab. Selbstverständlich ist es in vielen Fällen möglich, mit einem entsprechenden Vertrag die Eliminierung von Schwachstellen zu bewirken. Als Hilfsmittel für eine Schwachstellenabklärung kann beispielsweise eine Schwachstellenbewertungsliste eingesetzt werden, anhand derer für Cloud-Computing besonders empfindliche Schwachstellen bewertet werden können. Neben den auf Interviewbasis durchgeführten Schwachstellen-Abklärungen können durch den Kunden, vor einem Vertragsabschluss, auch für den Anwendungsfall spezifische Nachweise in der Form von Tests (z.B. Penetration Tests) oder Auditierungen durch unabhängige Instanzen verlangt werden.

Lösung zu Frage 4

Zu Ermittlung der Impacts wird der „Owner“ des durch das Cloud Computing zu unterstützenden Geschäftsprozesses konsultiert.

Lösung zu Frage 5

In der Evaluationsphase (Phase 2) wird eine Grobfassung des Sicherheitskonzepts mit den Anforderungen für die Provider-Evaluation durchgeführt. Aus dem bis dahin möglichen Risiko-Assessment sind dem Kunden in dieser Phase lediglich die „Worst Case Impacts" bekannt. Die konkreten Massnahmen können in dieser Phase lediglich ansatzweise bestimmt werden; diese können erst nach der Auswahl eines Providers konkret ermittelt werden. Aus der Impact-Analyse können jedoch bereits notwendige Grundschutz-Massnahmen ersehen werden, die bei der Schwachstellenuntersuchung und Auswahl eines Providers sicherlich hilfreich sind und deshalb in der Grobfassung des Sicherheitskonzepts aufgeführt werden sollten.

Lösung zu Frage 6

Für die Vertragsentwicklung wichtige Service-Management-Prozesse auf der Kundenseite sind:

- **Event Management**

  Das Event Management überwacht alle Ereignisse in einer IT-Infrastruktur, die eine Statusänderung zur Folge haben oder haben können. Somit dient es dem übergeordneten Ziel, den Normalbetrieb zu gewährleisten und bei Abweichungen koordinierte Massnahmen einzuleiten. Die Menge der Ereignisse die zu einem Incident führen (s. Incident Management), ist eine Teilmenge der durch das Event-Management feststellbaren und zu behandelnden Ereignisse. Anlauf- und Registrierungs- und Auftragsweiterleitungsstelle im Sinne eines Single Point of Contact (SPOC) könnte ein entsprechend eingerichtetes Service Desk sein.

- **Incident Management,**

  Das incident-Management nimmt sich vor allem den Sicherheitsvorfällen an. Solche Vorfälle können Ausfälle, Fehler oder relevante plötzlich erkennbare Schwachstellen (Vulerabilities oder Exploits) sein. Solche Vorfälle sollten über ein Service Desk oder eine ähnliche Anlauf- und Verwaltungsstelle gemeldet werden.

- **Request Fulfillment**

  Request fulfillment kümmert sich um Service Requests. Die Service Requests sind dabei Anforderungen die vor allem von der Benutzerseite her eingereicht werden (Solche Anforderungen können beispielsweise Softwareanpassungen oder der Wunsch für eine Änderung eines Zugriffsprofils sein.). Die Entgegennahme von Service Requests sollte auch über ein Service Desk erfolgen

- **Problem Management**

  Das Problem-Management hat die Aufgabe, sämtliche im Zusammenhang mit der Dienstleistung aufkommenden Probleme zu behandeln, dazu gehört, das Eintreten resp. das wiederholte Eintreten eines Vorfalls (Incident) zu verhindern sowie die Schadensauswirkungen eines dennoch eingetretenen Vorfalls möglichst gering zu halten.

- **Access Management (Zugriffverwaltung)**

  Durch das Access Management wird der Zugriff auf Ressourcen geregelt und die Verfahren zur Autorisierung von berechtigten Zugriffen durchgeführt und unberechtigte Zugriffe verhindert. Dafür verfügt das Access Management über entsprechende Benutzer- und Berechtigungs-Verwaltungsprozessen sowie Zugangs- und Sperrungsmechanismen.

Lösung zu Frage 7

Die Zuteilung und Kontrolle der Zugriffsberechtigungen der Benutzer auf die Applikationen in der Cloud obliegen der Verantwortlichkeit des Kunden. Die Berechtigungen auf Applikationsfunktionen, u.a. auf die Daten, muss der Kunde gemäss seinem Ermessen zuteilen können. Doch kann die Erfassung der Berechtigungen im System manchmal lediglich durch den Provider auf Anforderung des Kunden vorgenommen werden. Besonders in einem solchen Falle muss der Kunde die Möglichkeit haben, die erfassten Berechtigungen jederzeit zu überprüfen. Die Beauftragung für Berechtigungserfassungen sowie die im System tatsächlich erfassten Zugriffsberechtigungen (ob durch den Kunden selbst oder durch den Provider erfasst) müssen im Sinne einer sicheren Zugriffskontrolle nachvollziehbar sein.

Lösung zu Frage 8

Ein Sicherheitskonzept zwingt vor allem auf der Kundenseite zur Schriftlichkeit und damit auch zur Nachvollziehbarkeit des Assessment-Prozesses und der im Vertrag mit dem Provider letztendlich zu vereinbarenden Massnahmen. Wird das Sicherheitskonzept in der im Buch beschriebenen Struktur zuerst in einer Grobfassung und später in eine Detailfassung erstellt, dann kann es sämtliche Phasen eines Cloud-Computing-Projekt begleiten und eine schriftliche Dokumentation der Anforderungen und der jeweils zu verlangenden und letztlich vereinbarten Massnahmen darstellen. So enthält das Sicherheitskonzept in einer groben für die Evaluation massgeblichen Fassung ein Risiko-Assessment aus Sicht der Risikoobjekte (Assets) des Kunden, aus dem bereits in den Evaluationsprozess einfliessende Sicherheits-Anforderungen geschlossen werden können.