Med-Cloud-System

Umsetzung der Anforderungen der sicheren Verwendung eines externen CLOUD-Services - LEITLINIE

2. Präambel

Die Leitlinie 4U „Umsetzungshinweise für die sichere Verwendung eines CLOUD-Services in der SPENGER-KLINIK“ helfen die Sicherheitsanforderungen der Leitlinie 4A anzuwenden. Die Leitlinie A4 führt einen Prozess ein, mit dem sich Risiken der externen Cloud-Nutzung identifizieren, bewerten und behandeln lassen. Damit bleiben diese für Spenger-Klinik als Cloud-Kunde beherrschbar. Hierfür werden die Phasen Beschaffung, Einsatz und Beendigung von externen CloudDiensten betrachtet. Für jede Phase werden entsprechende Sicherheitsanforderungen zur Gewährleistung der Informationssicherheit aufgestellt. Die Sicherheitsanforderungen sind bereits in existierenden Standards, Normen und Regelungen als relevant identifiziert worden und sind daher den Cloud-Anbietern bereits bekannt. Eine ganz zentrale Bedeutung bei der Bewertung von externen Cloud-Diensten nimmt der, vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene, Anforderungskatalog Cloud Computing (BSI C5) ein. Die Leitlinie A4 greift die Themenkomplexe Informationssicherheit, Transparenz der CloudDiensterbringung und Nachweis über diese Aspekte durch geeignete Prüfungen auf. Rahmenbedingungen für die Cloud-Diensterbringung werden konkretisiert. Zudem wird vorgegeben, wie die Prüfnachweise des Cloud-Anbieters für das Informationssicherheitsmanagement der Spenger-Klinik genutzt werden sollen.

3. Umsetzungshinweise für die Sicherheitsanforderungen

Die Sicherheitsanforderungen teilen sich auf die Beschaffungs-, die Einsatz- sowie die Beendigungsphase von externen Cloud-Diensten auf.

A1 - Systembeschreibung und weitergehende Informationen fordern „Die Vorlage der Systembeschreibung des Cloud-Dienstes muss in der Leistungsbeschreibung gefordert werden. Sie muss die Vorgaben nach BSI-C5 erfüllen und ist insbesondere auf Mitwirkungspflichten (1) und Maßnahmen hin zu prüfen.

Zur Beurteilung des Cloud-Anbieters können weitergehende Informationen im Rahmen der Leistungsbeschreibung gefordert werden. Zudem sind mit Hilfe der Leistungsbeschreibung Basis- und Zusatzleistungen festzulegen.“

Zu (1): Mitwirkungspflichten bei Informationssicherheitsproblemen nehmen bei Cloud-Diensten eine wichtige Rolle ein. Die Anforderung soll daher entsprechend sensibilisieren und im Vertrag festgelegt werden.

4. Umsetzungshinweis für die Anforderung bei der Beschaffung des CloudServices (Vertrag)

4.1. Umsetzungshinweise für die Systembeschreibung des Anbieters

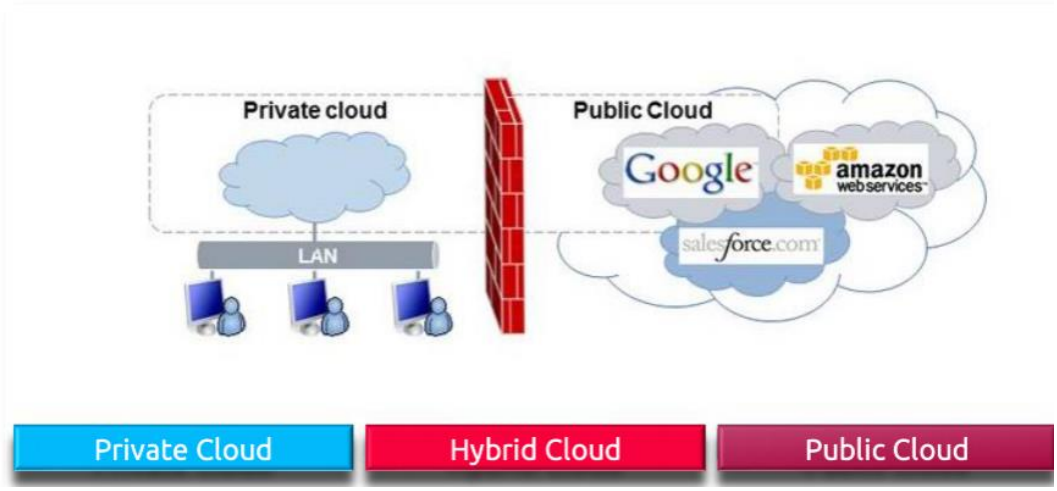
Der Cloud-Anbieter macht in seiner Systembeschreibung nachvollziehbare und transparente Angaben zum Cloud-Dienst, die es einem sachverständigen Dritten erlauben, die grundsätzliche Eignung des Cloud-Dienstes für die gewünschte Anwendung zu beurteilen. Die Systembeschreibung beschreibt die folgenden Aspekte:

» Art und Umfang der erbrachten Cloud-Dienste gemäß der Dienstgütevereinbarung (Service Level Agreements), die einem Vertrag mit den Cloud-Kunden typischerweise zugrunde liegt,

Partner: Med-Cloud-System und Spengerklinik

Umfang: Es soll eine Cloud eingerichtet werden, welche sowohl im Betrieb selbst, als auch außerhalb des Unternehmens zugriffsbereit ist. Diese soll jedoch vor unbefugten Zugriff von Dritten ausgeschlossen sein. Geeignet dafür wäre eine Hybrid-Cloud, welche sowohl als private- als auch als public-Cloud fungiert.

» Beschreibung der eingesetzten Infrastruktur-, Netzwerk- und Systemkomponenten für Entwicklung und Betrieb des Cloud-Dienstes,



Benötigt wird ein Router, welcher zwischen der privaten und der public-Cloud steht und für die Kommunikation nach außen zuständig ist. Für den Sicherheitsaspekt ist eine Firewall notwendig und soll vor Angriffen von außen schützen. Innerhalb des Betreibes arbeiten alle Clients im Local-Area-Network, wodurch Sie mit der private Cloud kommunizieren können.

In der Klinik wird außerdem ein Anbindung zum e-Card System benötigt (GINA).

» Umgang mit bedeutsamen Vorkommnissen und Verhältnissen, die Ausnahmen vom Regelbetrieb darstellen, wie bspw. der Ausfall von kritischen IT-Systemen,

Die Daten sollen rund um die Uhr verfügbar sein. Ärzte sollen in der Lage sein, Berichte während ihrer Home-Office-Zeit aus der Cloud herunterzuholen und neue Berichte hinzuzufügen. Außerdem ist die Klinik 24 Stunden im Betrieb weswegen das Service 24 / 7 benötigt wird.

Um das Risiko zum Verlust von Patientendaten zu minimieren, soll alle 15 min eine Sicherung aller Daten aus der Cloud gemacht werden und automatisch auf einem Server gesichert werden.

Bei Ausfall soll dieser als Backup dienen, damit zumindest nur die Daten von vor 15 min verloren gehen.

» Rollen und Zuständigkeiten des Cloud-Anbieters und des Cloud-Kunden, einschließlich Mitwirkungspflichten und korrespondierender Kontrollen beim Cloud-Kunden,

Bei Problematiken und unerwünschten Ereignissen sollte jederzeit eine Ansprechperson seitens des Anbieters zur Verfügung stehen, um rasch der Problematik entgegenwirken zu können.

In unserem Fall ist das:

a) DI Gerhard Frötzl, MSc
b) Vertretung: Ing. Karim Schöller

Seitens der Spengerklinik fungieren folgende Personen für die externe Firma als Ansprechpersonen:

a) Dr. Dr. Uni-Prof. Priv-Doz. Ingrid Semmler
b) Harald Dosnic, MSc

» an Unterauftragnehmer vergebene oder ausgelagerte Funktionen. Ergänzende Informationen zur Basisanforderung
//

Die Beschreibung der Infrastruktur-, Netzwerkund Systemkomponenten sollen so detailliert sein, dass der Cloud-Kunde einen guten und für Risikoabwägungen im Rahmen seines Sicherheitsmanagements notwendigen Überblick erhält ohne jedoch die Sicherheit des Cloud-Anbieters durch deren Darlegung zu gefährden

4.2. Umsetzungshinweise für die Zertifizierungen des Anbieters

Damit ein Anbieter als zuverlässig eingestuft werden kann müssen mindestens zwei der unten angeführten Zertifizierungen vorliegen:

- » ISO/IEC 27001 (ggf. auch auf der Basis von IT- Grundschutz)
- » ISO 22301
- » von den zuständigen Datenschutzbehörden akzeptierter Nachweis über die Einhaltung des Datenschutzes
- » Prüfberichte nach ISAE 3402/SSAE 16/SOC1/ IDW PS 951
- » Softwarebescheinigungen nach IDW PS 880

Zur Bestätigung auf Richtigkeit dieser Zeugnisse soll vor dem Vertrag ein externes Audit beim Anbieter stattfinden, bei der folgende Personen anwesend sein sollen:

- externer/externe Auditor/Auditorin, die eine weitere Zertifizierung ausstellt

- In unserem Fall ist das:
  - DI Gerhard Frötzl, MSc
  - Vertretung: Ing. Karim Schöller

- Seitens der Spengerklinik
    - Dr. Dr. Uni-Prof. Priv-Doz. Ingrid Semmler
    - Harald Dosnic, MSc

4.3. Umsetzungshinweise für die Sicherheitsnachweise des Anbieters

Basisanforderung Die Unternehmensleitung wird durch regelmäßige Berichte über den Stand der Informationssicherheit auf Grundlage der Sicherheitsprüfungen informiert und ist verantwortlich für die zeitnahe Behebung von daraus hervorgegangenen Feststellungen.

Interne Überprüfungen der Compliance von IT-Prozessen mit internen Sicherheitsrichtlinien und Standards Basisanforderung Qualifiziertes Personal (z. B. Interne Revision) des Cloud-Anbieters oder durch den Cloud-Anbieter beauftragte sachverständige Dritte überprüfen jährlich die Compliance der internen IT-Prozesse mit den entsprechenden internen Richtlinien und Standards sowie der für den Cloud-Dienst relevanten rechtlichen, regulativen und gesetzlich vorgeschriebenen Anforderungen. Die identifizierten Abweichungen werden priorisiert und in Abhängigkeit ihrer Kritikalität, werden Maßnahmen zur Behebung zeitnah definiert, nachverfolgt und umgesetzt.

Um dies zu Verwirklichen ist eine standardisierte Tabelle zu befüllen in der die Kritikalität zu dem jeweiligen Punkt evaluiert wird. Zudem sollen Maßnahmen angeführt werden, um die Risikostufe evtl. hinunterzusetzen. Sollte bei der Evaluierung ein Aspekt als hoch eingestuft werden, müssen die Maßnahmen sofort in Kraft treten und innerhalt von 2 Monaten in dem Zustand bringen, sodass beim nächsten Überprüfen die Kritikalitätsstufe maximal mittel ist.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit) Die Prüfung wird mindestens halbjährlich durchgeführt.
Zu dem Aspekt soll fortlaufend zumindest eine IT-Sicherheitsperson seitens der Anbieterschaft jederzeit Vorort sein (bzw. eingestellt werden), da die Sicherheit kein Zustand ist, sondern ein Prozess. Sollte ein Fehler auftreten (z.B. ein CIA-Triade wurde verletzt → Verfügbarkeit ist nicht gewährleistet, Daten in der Cloud wurden manipuliert, Unbefugte Personen haben Zugriff auf die Daten, etc.) kann die zuständige Person sofort Maßnahmen setzen und der Verletzung entgegenwirken. Aufgrund der Tatsache, dass es sich um personenbezogene Patientendaten handelt, ist das Gesundheits-Risiko der Individuen sehr hoch, weswegen sofortiges Einschreiten von höchster Bedeutung ist.

Die Prüfung umfasst auch die Einhaltung der Anforderungen dieses Anforderungskatalogs.

Interne Überprüfungen der Compliance von IT-Systemen mit internen Sicherheitsrichtlinien und Standards

4.4. Umsetzungshinweise für die Beendigung des Vertragsverhältnisses regeln

Bei der Beendigung des Vertragsverhältnisses erfolgt eine vollständige Löschung der Inhaltsdaten des Cloud-Kunden, einschließlich der Datensicherungen und der Metadaten (sobald diese für die ordnungsgemäße Dokumentation der Abrechnung nicht mehr benötigt werden). Die hierzu eingesetzten Methoden (z. B. durch mehrfaches Überschreiben der Daten, löschen des Schlüssels) verhindern eine Wiederherstellung mit forensischen Mitteln.

Um dies zu erfüllen, werden sowohl der Back-Up Server, der alle 15min syncronisiert wird mit der Cloud komplett bereinigt, als auch die belegten Speicherzellen auf der Cloud. Der Server soll komplett formatiert werden um keine Datenreste zu hinterlassen, der Server auf der die standardmäßige Cloud rennt, soll einmal komplett gesäubert werden.

5. Umsetzungshinweise für die Anforderungen beim Beendigen des Cloud-Services