Med-Cloud-System

Anforderungen der sicheren Verwendung eines externen Cloud-Services - Leitlinie

2. Präambel

Die Leitlinie 4A „Anforderungen für die sichere Verwendung eines CLOUD-Services in der SPENGERKLINIK“ definiert die Sicherheitsanforderungen an die Nutzung eines solchen Services. Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IKT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Insbesondere werden dabei Infrastrukturen, Plattformen und Software angeboten, die Spannbreite der angebotenen Cloud-Dienste umfasst darüber hinaus jedoch das komplette Spektrum der Informationstechnik. Externe Cloud-Dienste im Sinne dieser Leitlinie sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netzwerke und Anbieter der Wirtschaft außerhalb der Spenger-Klinik erbracht werden.

3. Sicherheitsanforderungen

Nachfolgende Sicherheitsanforderungen adressieren die Beschaffungs-, die Einsatz- sowie die Beendigungsphase von externen Cloud-Diensten. Diese sind einzuhalten, um ein Mindestmaß an Informationssicherheit zu gewährleisten. Sie können jedoch bei Bedarf durch zusätzliche Anforderungen erweitert werden. Vor der Nutzung externer Cloud-Dienste ist zusätzlich zur Schutzbedarfsfeststellung eine vorgelagerte Datenkategorisierung und Risikoanalyse durchzuführen.
Im Rahmen der Datenkategorisierung der Vertraulichkeit sind die Daten den nachfolgenden Klassen
zuzuordnen:

Öffentlich ... (ergänzen),
Vertraulich ... (ergänzen),
Geheim ... (ergänzen)

A1: Systembeschreibung des Anbieters
A2: Zertifizierung des Anbieters
A3: Sicherheitsnachweise des Anbieters
A8: Beendigung des Vertragsverhältnisses regeln

4. Anforderung bei der Beschaffung des Cloud-Services (Vertrag)

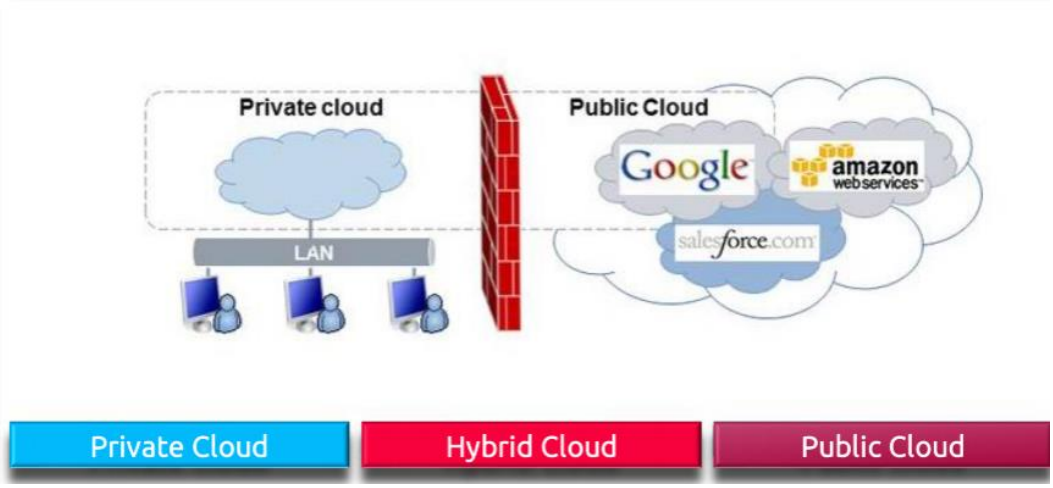
4.1. Systembeschreibung des Anbieters

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.

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



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.

» 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.

» 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. Zertifizierung 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

4.3. 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. „ SPN-02 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.

Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit) Die Prüfung wird mindestens halbjährlich durchgeführt.

Die Prüfung umfasst auch die Einhaltung der Anforderungen dieses Anforderungskatalogs.

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

Basisanforderung Qualifiziertes Personal (z. B. Interne Revision) des Cloud-Anbieters oder durch den Cloud-Anbieter beauftragte sachverständige Dritte überprüfen mindestens jährlich die Compliance der IT-Systeme, soweit diese ganz oder teilweise im Verantwortungsbereich des Cloud-Anbieters liegen und für die Entwicklung oder den Betrieb des Cloud-Dienstes relevant sind, 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. Optionale, weitergehende Anforderungen (Vertraulichkeit und Verfügbarkeit) Auf Anfrage der Cloud-Kunden stellt der Cloud-Anbieter Informationen über die Ergebnisse, Auswirkungen und Risiken dieser Prüfungen und Beurteilungen in angemessener Form zur Verfügung. Der Cloud-Anbieter verpflichtet seine Unterauftragnehmer zu solchen Prüfungen und lässt sich die Prüfberichte im gleichen Turnus vorlegen und verwertet sie bei seinen Überprüfungen.

4.4. 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.