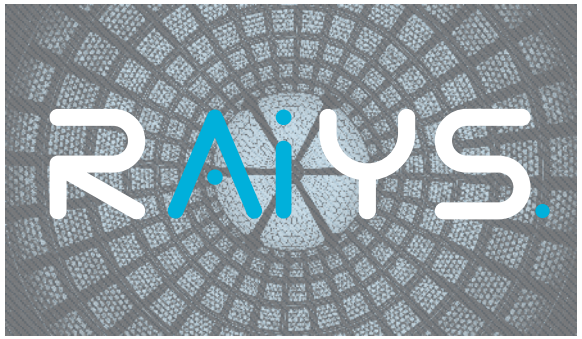
Praxis-IT in der Cloud

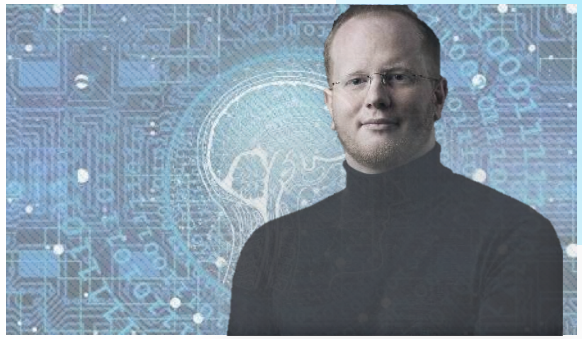
Offenlegung von Interessenkonflikten

Hiermit erkläre ich, dass zu den Inhalten der Veranstaltung
ein materieller Interessenskonlfikt vorliegt.

Unternehmen	Verbindung / potenzieller Konflikt
Raiys GmbH	Beschäftigungsverhältnis

About us





Mission & Vision

Unsere intelligente, auf KI basierende Software ist der Schlüssel zur Bewältigung der wachsenden Datenmengen in der Zukunft.

Raiys GmbH

Seit der Gründung im Jahr 2021 ist es unser Bestreben, Ärzten dabei zu helfen, Patienten zu helfen.

Dominik Wolf

Software-Architekt, Cloud-Native in der Praxis, umfassende Erfahrung im hochreguliertem Umfeld seit 2016.

Patienten sind bereits in der Cloud,
Dienstleister sind bereits in der Cloud,
das fehlende Bindeglied sind radiologische Praxen.

DoctoLib - wird gehostet via Cloudflare [1]

Nelly - wird gehostet in der Amazon Cloud [2]

Allianz SE - ging bereits 2019 eine Partnerschaft mit Microsoft ein [3]

Siemens Healthineers - migriert zu einer Cloud Lösung [4]

[1] doctolib.de CLOUDFLARENET – 23.04.2024

[2] patient.gonelly.de AWS EC2 (eu-central-1) - 23.04.2024

[3] Allianz und Microsoft gehen Partnerschaft für digitale Transformation der Versicherungsbranche ein – 14.11.2019

[4] Siemens Healthineers migriert in die Cloud - 25.10.2023

Was bringt die Zukunft?

Wir befinden uns in bewegten Zeiten.
Einerseits technologische Innovationen, KI-gestützte Bildanalyse.
Andererseits aktuelle und künftige Herausforderungen wie steigende Daten- und Informationsflut, politische und juristische Änderungen.

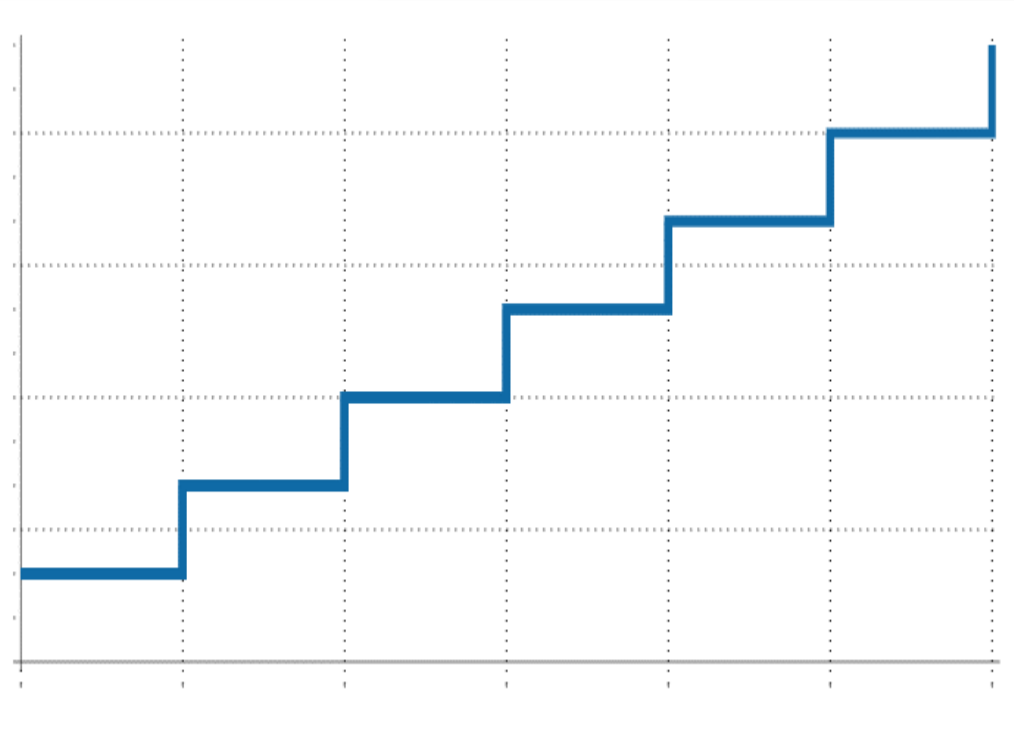
Aktuelle Herausforderungen

01 Hardware-Skalierung

Kosten

- **Hohe Anschaffungskosten** – eingeschränkte Skalierung durch teure Systeme
- **Kaum Austauschsysteme** – im Fehlerfalle ist die Hardware oft nicht 1:1 zu ersetzen
- **Ungenutzte Hardware** – durch tendenziell initial großzügigere Planung inkl. Puffer

Visualisierung Kostensprünge Hardware



02 Backups und Archivierung

- **Aufbewahrung** - Backups selten in einer Brandschutzzone
- **Redundanz** – Meist keine geo-redundante Aufbewahrung
- **Einspielzeit** - die Einspielzeit der Backups wird oft nicht mitgedacht, häufig beträgt diese ***Tage***, vollständige Wiederherstellung des Archivs kann ***Wochen*** betragen
- **Verschlüsselung** - Backups meist nicht verschlüsselt

03 Sicherheit

- **Mangelhafte Isolation** – häufig laufen mehrere Systeme auf der gleichen Umgebung ohne Containerisierung
- **Keine IPS und IDS*** – Systeme zur Prävention, Musterkennung & Alarmierung sind in der Regel nicht im Einsatz
- **Unverschlüsselte interne Netze** – eine erfolgreiche Attacke vor Ort reicht aus, um Traffic mitzulesen
- **VPN als Workaround** – ein kompromittiertes System kann genutzt werden, um weitere Systeme zu infizieren
- **Audit Log** – wenn vorhanden, über mehrere Systeme verteilt

* IPS = Intrusion Prevention System; IDS = Intrusion Detection System

04 Wartung und Aktualisierung

- **Fehleranfälliges Updaten** – oft besteht bei System-Updates keine Möglichkeit für einen “einfachen” Rollback
- **Kein Testbetrieb möglich** – neue Features können nicht wenigen Geräten vorab getestet werden; ein Rollout betrifft stets alle Einheiten
- **Unzureichend gewartete Systeme** – von außen erreichbare Systeme, z.B. Patienten-Portale oder Mailserver, sind Angriffsvektoren
- **Steigende Komplexität** – Anzahl der genutzten Systeme steigt, hierdurch sind Fehlkonfigurationen und Wechselwirkungen wahrscheinlicher

Welche Lösungen bietet die Cloud?

01

Hardware-Skalierung

- **Keine Kostensprünge** - Neuanschaffung von Hardware entfällt durch Auslagerung.
  Die Kostenabschätzung kann linear erfolgen.

- **Bedarfsgerechte Ausstattung** - Puffer für die Systeme muss nicht direkt vorgeplant werden, es kann bei Bedarf zu- und abgeschaltet werden.

- **Kosteneinsparung -** Storage Systeme können in heiße, kalte und Archiv-Zugriffsebenen unterteilt werden.
  Keine Vorhaltung von Austauschsystemen und Austauschplatten.

02

Backups und Archivierung

- **Aufbewahrung und Redundanz -** Backups werden standardmäßig mindestens in einer anderen Brandschutz-Zone vorgehalten, können per Knopfdruck in andere Locations verschoben werden.
- **Einspielzeit -** Backup Systeme bereitstellen ist eine Sache von Minuten bis Stunden und nicht mehr von Tagen oder Wochen.
- **Verschlüsselung –** einfach zuschaltbar.

03

Sicherheit

- **Isolation –** Systeme werden in isolierten Containern betrieben und sind nur über Schnittstellen erreichbar.
- **IPS und IDS -** Intrusion Detection und Intrusion Prevention Systeme können vorgelagert werden, ohne die Infrastruktur neu planen zu müssen.
- **Verschlüsselte Netze -** die Verbindung zu den Systemen ist mindestens TLS verschlüsselt.
- **Audit Log –** Audit Logs können für alle Systeme zentral gespeichert und ausgewertet werden.
- **VPN als Workaround –** VPN-Netze werden größtenteils obsolet. Dies reduziert den zu verwaltenden Overhead.

04

Wartung und Aktualisierung

- **Updates –** Updates werden durch Containerisierung zurückrollbar.
- **Testbetrieb –** isoliertes Hochfahren von neuen Features in einem neuen Container ist problemlos möglich.
- **Wartung –** durch die Auslagerung des Hostings entfällt ein Großteil der teils aufwändigen Infrastruktur-Updates, Software kann in der Regel komplett automatisiert aktuell gehalten werden.
- **Synergieeffekte –** Zentrale Verwaltung der Systeme und Updates. Sicherheitsstandards immer im Überblick.

Ist die Cloud immer besser?

Prinzipiell schon – es gibt aber Fallstricke.

Wie schaffe ich es, sicherzustellen, dass mein Dienstleister nicht auf meine Verschlüsselung zugreifen kann?

- Die Finanzbranche macht es vor – es ist kompliziert, aber best practice. “Bring Your Own Key”, abgesichert über Hardware Security Module. Durch diese ***manipulationssichere*** Technik kann das Prinzip des Schlüsselentzugs und der Unbrauchbarmachung von Daten umgesetzt werden.

Wie sichere ich besonders kritische Systeme in der Cloud?

- Durch die Nutzung von 2FA, RBAC, IP Whitelists und selbstverständlich auch VPN können weitere Sicherheitsmaßnahmen ***passgenau*** und ***bedarfsgerecht*** ergriffen werden.

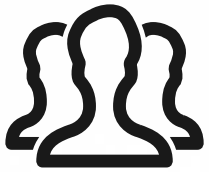
MEHRWERTE FÜR RADIOLOGEN

Kollaboration, Austausch und Synergieeffekte

KONSIL

Sichere Datenübermittlung
ohne Zeitverzögerung

Die Bilder können von überall und auf jedem Gerät mit Internetzugang sicher abgerufen werden, was die Zusammenarbeit und den Austausch von Bildern erleichtert.



AUSTAUSCH

Nutzerfreundliches, gemeinsames
Bild-Archiv

Bessere Diagnostik durch mehr Vergleiche in einer größeren Datenbasis, einrichtbar mit mehreren Freigabestufen, anonyme Bilder oder mit Patientendaten.

SYNERGIEN

Weniger Aufwand
durch best practices

Schaffung von best practices des RG-Kollegiums erlaubt es Einzelnen, mit weniger Aufwand Rechtssicherheit zu schaffen, neue Rechts-normen standardisiert umzusetzen, Aufklärung der Patienten zu erleichtern.

Wie geht es weiter?

Quo vadis?

Aktiv werden … für Ihre Zukunft

**Allianzen bilden –
Synergien erzeugen**

**Politisches Gewicht
schaffen –
für Zukunftssicherheit**

**Überholte Systeme
ändern –
für mehr Flexibilität**

**Neue Strukturen
aufbauen –
für mehr Sicherheit**

Vielen Dank

Für Ihre Fragen stehen wir Ihnen gerne zur Verfügung.