Risikomanagement und Datensicherheit der KIS

Datensicherheit in den DRK Kliniken Berlin

Das Konzept der „fernen“ Datensicherung

Michael Thoss
Leiter Zentrale Dienste Organisation und IT
DRK Kliniken Berlin

Infrastrukturgrundlagen

- Einheitliche KIS auf einheitlicher UNIX-Plattform
- Homogene IT-Infrastruktur auf wenigen Produktlinien
- Client/Server-Architektur mit Softwareverteilung
- Homogene integrierte Softwarelandschaft mit wenigen Subsystemen (Ziel EPA)
- LAN als Gigabit-Ethernets für u.a. PACS-Applikation
- WAN als VPN (IPSec) mit Einwahloptionen, Internetzugang
- Kommunikation für §301/302
- Kommunikation über Carrier und Standardplattformen
- Externe redundante Datensicherung im DataCenter
- IT und Medizinische Informatik für Projekt- und Systembetrieb mit 19 Mitarbeitern

Ausgangsszenario

- Ungenügende Raum-Infrastruktur der verfügbaren Serverraum-Standorte
- Risikolasten im Umfeld der Rechenzentren
- Risikomanagement-Aufgaben (KontrAG, Basel)
- Datensicherheitsbedürfnisse (physikalisch)
- Datenschutzbedürfnisse (logisch)
- Investitionsmöglichkeiten und –relationen
- Gewichtung der Aufgabenstellungen
- Gewichtung der Risikopotentiale

Infrastruktur Serverräume

- Bestandsräume

  Krankenhäuser nutzen i.d.R. analog Kaufhäusern Flächen in erster Linie für die Leistungserbringung. Somit bleiben für technische Installation oftmals nur Bereiche in nicht idealer Ausprägung

- Sub-Optimale Situationen durch Lage und Infrastruktur wie z.B. Brandlasten, Wasserleitungen

  Daraus resultierend sind Infrastrukturmaßnahmen in geeigneter Qualität nur mit beträchtlichem Mitteleinsatz zu realisieren

Beispiel (Serverraummängel, Auszug)

- **Platzprobleme**
  Server, Speicher, Klima und USV im gleichen Raum
- **Lage**
  1. OG eines 8-geschossigen Gebäudes
  Oberhalb der zentralen Wäscheversorgung
  (Brandlasten unter und über dem Standort)
- **Infrastruktur**
  Tw. Versorgungsleitungen Wasser und Klima im Raum
- **Brandschutz**
  Nur Standards wie F90 (d.h. Menschen geschützt, IT-Anlagen jedoch nur bedingt), kein eigener Brandschutzbereich
- **...**

Ausgangspunkte

- Analyse der vorhandenen Infrastruktur an Serverräumen (Sicherheitsanalyse durch externen spezialisierten Dienstleister)
- Erstellung eines Maßnahmenplanes zur internen Risikoreduzierung
- Bewertung der notwendigen Mittelaufwendungen
- Überprüfung alternativer (Teil-)Szenarien
- Zweiteilige Konzeption zum Outtasking von Teilfunktionen (hier Online-Backup) und zur baulichen Härtung der Bestandsräume

Risikomanagement

- Gemäß der Risikomanagementaufgaben des Unternehmens sind die zentralen betriebswirtschaftlichen Systeme (KIS) zur Unterstützung der klinischen und administrativen Aufgaben in der Ereignis und Schadenhöhe-Kombination als kritisch einzustufen
- Ein mehrtägiger Systemausfall oder gar Datenverlust führt sowohl zu betriebswirtschaftlichen Folgen (Verlust von Abrechnungsinformationen) als auch zu Prozessfolgen (Verlust von Dokumentationsinformationen)
- Die Folgekosten aus Wiederherstellung und notwendiger Nacharbeit nehmen schon bei kurzen Zeiträumen beträchtliche Dimensionen an
- Die Integration immer weiterführender Prozessunterstützung auf IT-Plattformen entlastet zwar im Tagesgeschäft Ressourcen, führt aber beim Ausfall der Systeme zu vervielfachtem Aufwand

Datensicherheit (physikalisch)

- Grundsätzlich sind ernsthafte physikalische Schadenereignisse statistisch selten aber eben nicht unmöglich
- Prinzipiell erfüllen die wenigsten Raumstrukturen die physikalischen Bedingungen zum Schutz hochwertiger IT-Anlagen (Normen wie F90 nicht ausreichend)
- Oftmals sind auf Grund der Infrastruktur-Rahmenbedingungen nicht einmal separate Brandschutzzonen realisierbar
- Das Risiko des Datenverlustes von aktuell laufenden Sicherungsbändern ist immer gegeben und nimmt durch die Roboterhandhabung mit höherem Speichervolumen noch zu
- Datenschutzsafes bieten jeweils nur eine Stichtagssicherheit für Medien die nicht in aktuellem Gebrauch sind
- Die Sensibilität der Anlagen nimmt proportional zur Leistung zu

Datenschutz (logisch)

- Der logische Datenschutz stellt ein intern zu lösendes Problem dar, ist i.d.R. aber sachgerecht gelöst
- Der Datenschutz intern gelagerter Daten (Medien wie Bändern, Disks) im Hause ist kein logisches Problem
- Der Datenschutz extern gelagerter Daten (Datenbanken, Medien) stellt für Krankenhäuser ein datenschutzrechtliches Problem dar
- „Managend Services“ sind in erster Linie unzulässig, da dritten Zugriffsmöglichkeiten auf Unternehmensdaten möglich wären
- Regelungen sind lösbar

Datenschutzauflagen

- „Auftragsdatenverarbeitung“

  Der Zugang Dritter auf personenbezogene Daten des Unternehmens (im Krankenhaus: Patientendaten) ist untersagt. Jede Möglichkeit eines Auftragnehmers in diese Richtung stellt eine Auftragsdatenverarbeitung dar

- „Beschlagnahmeschutz“

  Patientenbezogene Daten unterliegen nur auf dem Gelände des Unternehmens dem gesetzlichen Beschlagnahmeschutz

Datensicherheitskonzept

- **Status**
- Lokale / Standortbezogene Datensicherungen in klassischer Generationenorganisation mit Tape-Librarys (täglich 1x voll zzgl. Inkrementeller Sicherung von z.B. DB-ReDoLogs)
- Lagerung der Medien in Safes der Klasse S 120
- Zyklische Prüfung der Medien (ggf. Austausch)
- Tägliche Kontrolle der Datensicherungsvorgänge
- **Erweiterungsplanung**
- Integration Online-Backup
- Datenhaltung Backup an fernem Standort
- Backup-Systemhaltung im Datacenter
- Integration in WAN (VPN/IPSec)

Data-Center Ansatz

- Verfügbare (Bestands-)Ressourcen (Räume, Anlagen) im eigenen Hause (Klinik) bilden i.d.R. nur den ohnehin vorhandenen baulichen und sicherheitstechnischen Standard ab
- Zukauf von Standards der Datensicherheit auf höchstem Niveau (Brandschutz, usw.)
- Günstiger verteilte Kosten (Vielzahl Nutzer)
- Minimale Investitionskosten des Kunden
- Seltener Zugangsbedarf an eine Online-Backup-Lösung (Keine Datenträgerwechsel, remote-Service)
- Datenschutzrechtliche Probleme ohne managed services lösbar

Vergleich „Make or Buy“

- **Intern (make)**
- Zusätzlicher Flächenbedarf
- Ggf. Erschließungskosten (Netzanbindung)
- Hohe Investitionskosten (Sicherheit, Energie, USV, Klima)
- Laufende Kosten
- Instandhaltungskosten
- Netzintegration (LAN)
- Begrenzte Sicherheit
- Bedingte Betriebssicherheit

- **Extern (buy)**
- Kalkulatorische Fläche
- Keine Erschließungskosten (Netzanbindung)
- Minimale Investitionskosten (Anschluß, einmalige Inbetriebnahme)
- Niedrige laufende Kosten
- Keine Instandhaltungskosten
- Netzintegration (WAN)
- Höchste Sicherheit
- Höchste Betriebssicherheit

Fazit

- Die DRK Kliniken Berlin haben sich für die Realisierung ihrer Backuplösung mit der STEAG Energie-Contracting GmbH (SEC) entschieden.
- Grundlage war die Umsetzung eines auf Krankenhausbetriebe angepassten Vertragswerkes
- Im Vordergrund standen jedoch die Vorteile eines unter Sicherheitsaspekten optimalen Systembetriebes ohne Erstellung eigener Ressourcen und unter Vermeidung hoher Investitionskosten
- Optional bietet sich aus den Erfahrungen die Möglichkeit sensible Serverressourcen perspektivisch ebenfalls in eine Hochsicherheitsumgebung umzulagern
- Die Bereitstellung eigener physikalischer Ressourcen in entsprechender Qualität ist wirtschaftlich aufwendiger