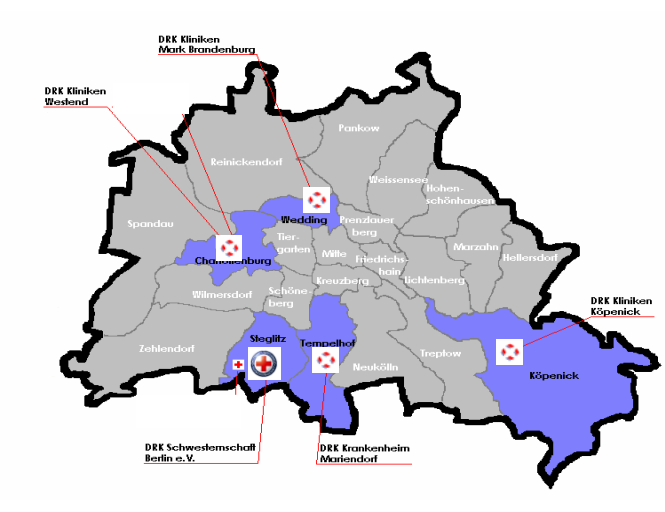
Institute for International Research

DRK Kliniken Berlin

Willkommen



Institute for International Research

DRK Kliniken Berlin

„Sicherheitsarchitekturen“

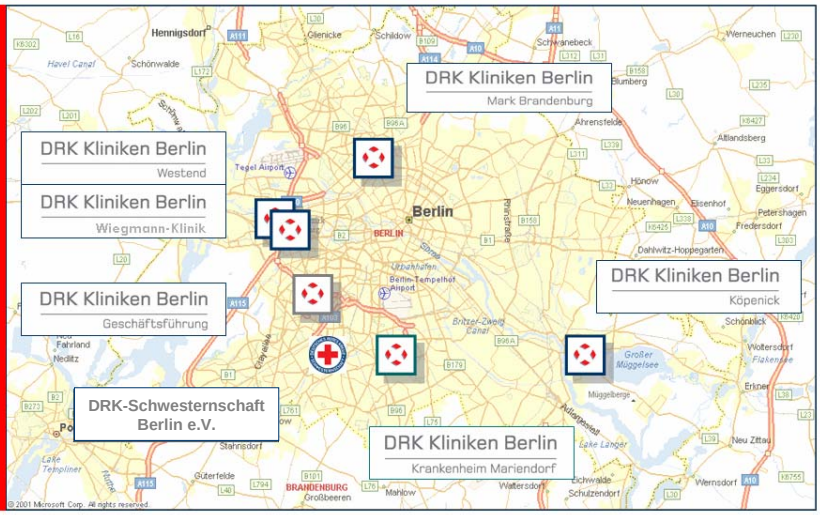
Komplexe Modelle für Sicherheits-architekturen und (Vorschläge für) Lösungsansätze bis hin zu Sicherheitschecks

Michael Thoss
Leiter Zentrale Dienste Organisation und IT
DRK Kliniken Berlin

Einrichtungen der
DRK-
Schwesternschaft
Berlin e.V.

DRK Kliniken Berlin

Standorte der DRK Kliniken Berlin



Institute for International Research

DRK Kliniken Berlin

Ein paar Zahlen

Akutbetten	1300
Pflegeplätze	160
Mitarbeiter	3000
ca. am System	2500
Arbeitsplätze	1200

(IT-) Zahlen

- 1200 Arbeitsplätze (PC) bei 1300 Betten
- Zusätzliche 160 Pflegebetten
- Weitgehende Prozessunterstützung (ohne Pflege)
- Ca. 3000 Mitarbeiter (2500 Vollzeit)
- Ca. 2500 Benutzer an den Systemen
- Ca. 1000 E-Mail-Nutzer
- Ca. 500 Internetnutzer
- Ca. 250 Arbeitsplätze (1/5) mit Wechselmedien
- Ca. 250 Arbeitsplätze (1/5) mit Zusatzfunktionen
- = 500 Arbeitsplätze mit Risikopotentialen

gGmbH‘s mit zentralen Bereichen

- Verwaltung
  - Personalabteilung
  - Rechnungswesen
  - Controlling
  - Einkauf & Apotheke
  - **Organisation & IT**
  - Qualitätsmanagement
  - Technik
  - Rechtsabteilung
  - Med. Controlling
  - Med. Informatik
  - Zent. Problemfall Man
- Medizin
  - Anästhesie
  - Pathologie
  - Labor
  - Hygiene
  - Ethik
  - Qualität (EFQM, JCIA)
- Zentrales Pflegemanagement
  - Bildungszentrum für Pflegeberufe

Infrastrukturgrundlagen

- Einheitliche KIS auf einheitlicher UNIX-Plattform (SOLARIS)
- Homogene IT-Infrastruktur auf wenigen Produktlinien (SUN/HP)
- Client/Server-Architektur mit Softwareverteilung (NoName)
- Homogene integrierte Softwarelandschaft mit wenigen Subsystemen (Ziel EPA). Ein Prozesstool für KIS/RIS/PACS
- 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
- RAS für RB und Fremdfirmen (SW und HW inkl. MPG, CT, etc)
- Externe redundante Datensicherung im DataCenter
- Zentraler Internetzugang, zentrale Security-/Contentlösung
- IT und Medizinische Informatik für Projekt- und Systembetrieb mit 21 Mitarbeitern

Sicherheit

- Man sollte es an Einstein anlehnen:

„Alles ist relativ“

„Ansichten und fehlende Einsichten… (Internet)“

- Leitende Angestellte…:

  „…Rechner stellen lediglich ein Arbeitsmittel dar, auf welches Mitarbeiter der Kliniken entsprechend ihren Aufgaben uneingeschränkt Zugriff haben müssen…“

  „… die für uns alle heutzutage essentiellen Arbeitsmittel unkompliziert zur Verfügung zu stellen…“

- …und höher…:

  „…langsam reicht es mir mit Ihrem webwasher…“

„Ansichten und fehlende Einsichten… (Internet)“

Aus dem Mailverkehr der Hotline:

„…ich habe entdeckt, es scheint ein neues spaßiges Spiel zu geben: "Finde selbst heraus was geht!" (oder auch nicht)
Heute habe ich herausgefunden, dass man Dateien mit dem Attachment .RAR ein äußerst gebräuchliches Format für komprimierte Dateien (und wesentlich mächtiger als .ZIP) nicht per Outlook versenden kann…“

Institute for International Research

DRK Kliniken Berlin

Technische Funktionskomponenten

Was gehört eigentlich alles zur Sicherheit?

Einrichtungen der DRK-Schwesternschaft Berlin e.V.

Institute for International Research

DRK Kliniken Berlin

Kennen Sie ihre Services?

- Alle Unternehmensservices z.B: TK, MedTech, u.a.
- Schwerpunkt: IT-Services
- (Neue) Anforderungen wie VPN, Portale (Zentrenbildung, integrierte Versorgung)
- Interne Services wie Rufbereitschaften, Heimarbeitsplätze, RAS, etc.
- „Versteckte“ Services (unbekannte Kopplungen zu Beispiel an Medizintechnischen Geräten, ISDN-Wartungszugänge, u.v.m.)
- Aber auch: PDAs und PDA-Handys
- Diensthandys

Bereitstellung Services der IT (1)

- KIS/RIS-Primärbetrieb
- KIS-Betriebswirtschaftliche Funktionen
- PACS-Primärbetrieb
- Primärbetrieb Krankenheim (Verwaltung/Pflege)
- Netzwerkbetrieb WAN (alle Standorte, VPN, IPSec)
- Netzwerkbetrieb LANs (alle Standorte, Gigabit-Eth.)
- Sekundärsystembetrieb (Exchange, Mail, Internet)
- Subsystembetrieb
- Serverbetrieb UNIX-Systeme (KIS/RIS)
- Serverbetrieb LINUX-Systeme (PACS)
- Serverbetrieb Windows-Systeme

Bereitstellung Services der IT (2)

- Serverbetrieb div. Abteilungs- und sonstige Subsysteme, (Windows) z.B.:
  - Diagnoseverschlüsselung
  - Arzneimittelindex
  - Verwaltung Medizin- und Betriebstechnik
  - Schülerverwaltung/Lehrpläne Krankenpflegeschule(n)
  - Anästhesiedokumentation
  - Perinataldokumentation
  - Tumordokumentation
  - Küchensystem (Catering)
  - E-learn-Plattformen

Bereitstellung Services der IT (3)

- Security-Services (Firewall, Scanner, Content)
- Datensicherheits-Services (BackUp, Recovery)
- Online-Backup im externen Data-Center
- Datenschutz-Services (Zugangsschutz, etc.)
- Kommunikation (§301 und §302)
- Kommunikation BGs, Praxen, etc.
- Kommunikation Subsysteme / SSt. (Komm.-Server)
- Störungsmanagement
- Problemmanagement
- Change-Management
- Release-Management (ORBIS und Subsysteme)
- Konfigurationsmanagement (alle Systeme)

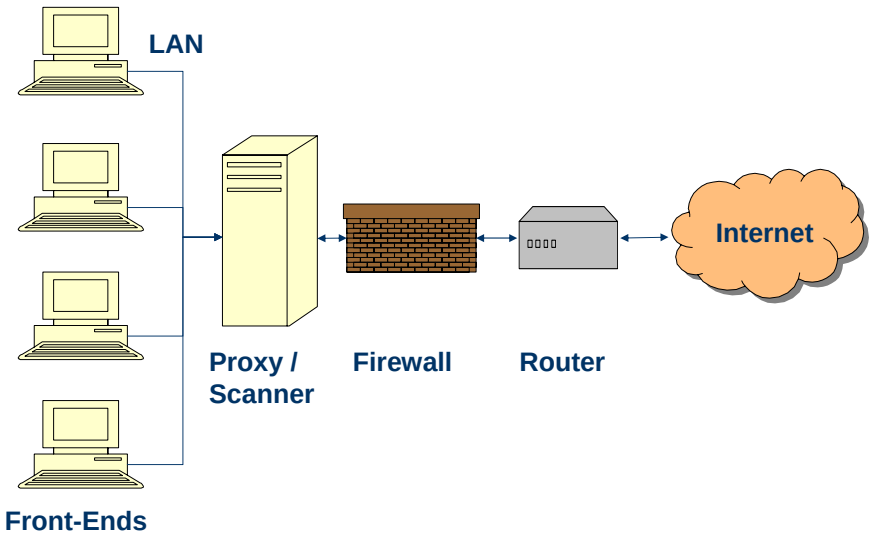
Bereitstellung Services der IT (4)

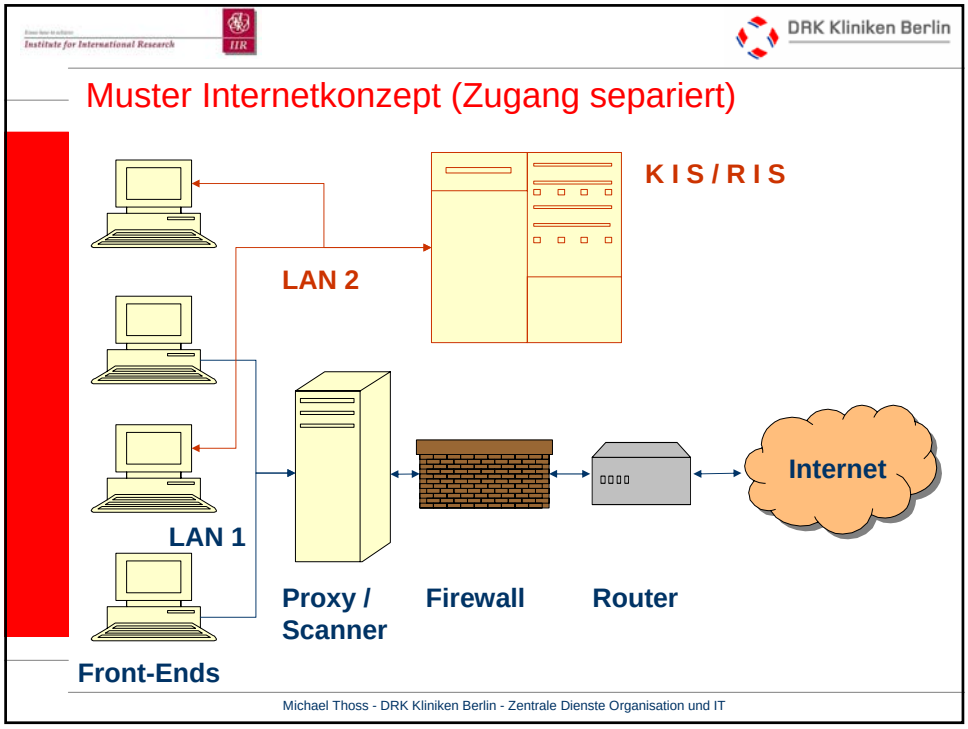
- File-Services (Gruppenlaufwerke)
- Instandhaltung Peripheriesysteme
- Front-End-Betrieb (ca. 1200 Einheiten)
- Druckerbetrieb (Laser und Formulardrucker, 600)
- Peripheriebetrieb (Monitore, Scanner, Zubehör, PDA)
- Hotline-Betrieb Benutzer (Remoteunterstützung)
- Schulungsangebote (Präsenzkurse, elearn)
- Stammdatenverwaltung / Benutzermanagement
- RAS-Dienste Servicepartner (inkl. MedTech)
- Internet- und Email-Betrieb

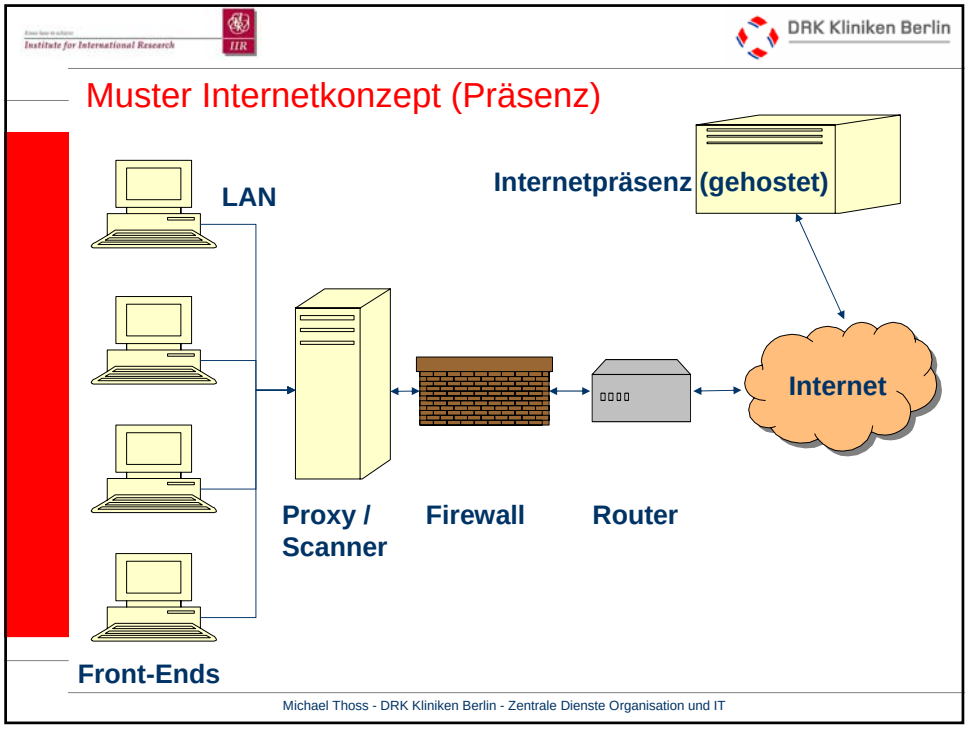
Bereitstellung Services der IT (5)

- Zunehmende Lasten durch:
- Systemintegration (Modalitäten)
  - Medizintechnik:
    - Radiologiemodalitäten
    - Sonstige Untersuchungstechnik (z.B. Ultraschall)
- Serviceintegration (Fernwartungsdienste)
  - Medizintechnik:
    - Radiologische Geräte
    - Labortechnik
    - Sonstige Untersuchungstechnik (LHK, etc.)

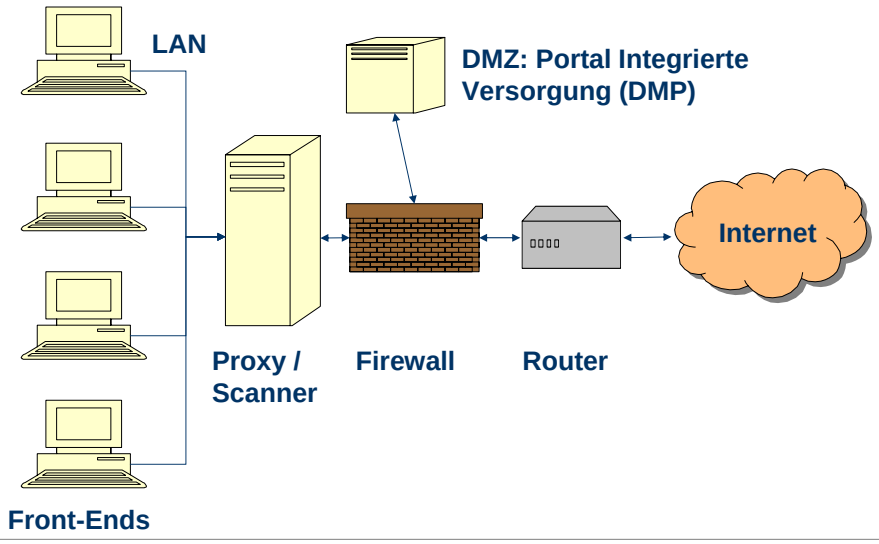
Muster Internetkonzept (Zugang)



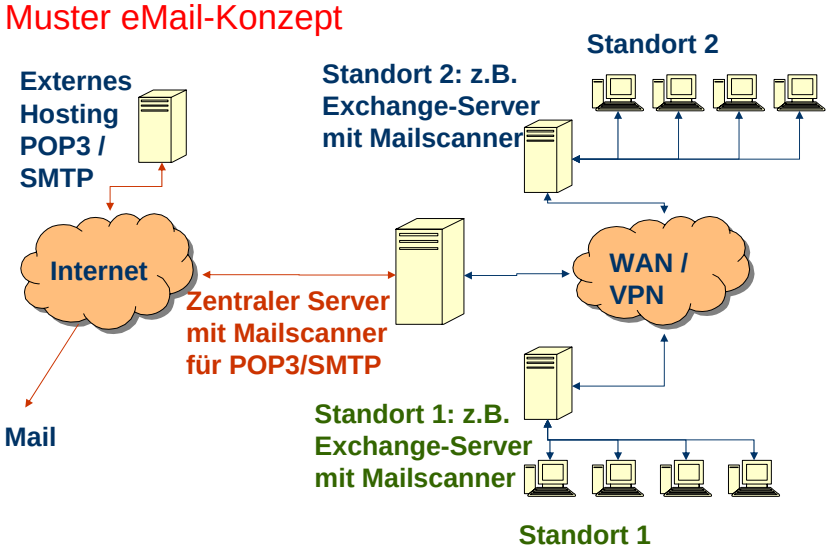

Institute for International Research
IIR
DRK Kliniken Berlin
Muster Internetkonzept (Zugang separiert)
K I S / R I S
LAN 2
LAN 1
Internet
Proxy /
Scanner
Firewall
Router
Front-Ends
Michael Thoss - DRK Kliniken Berlin - Zentrale Dienste Organisation und IT

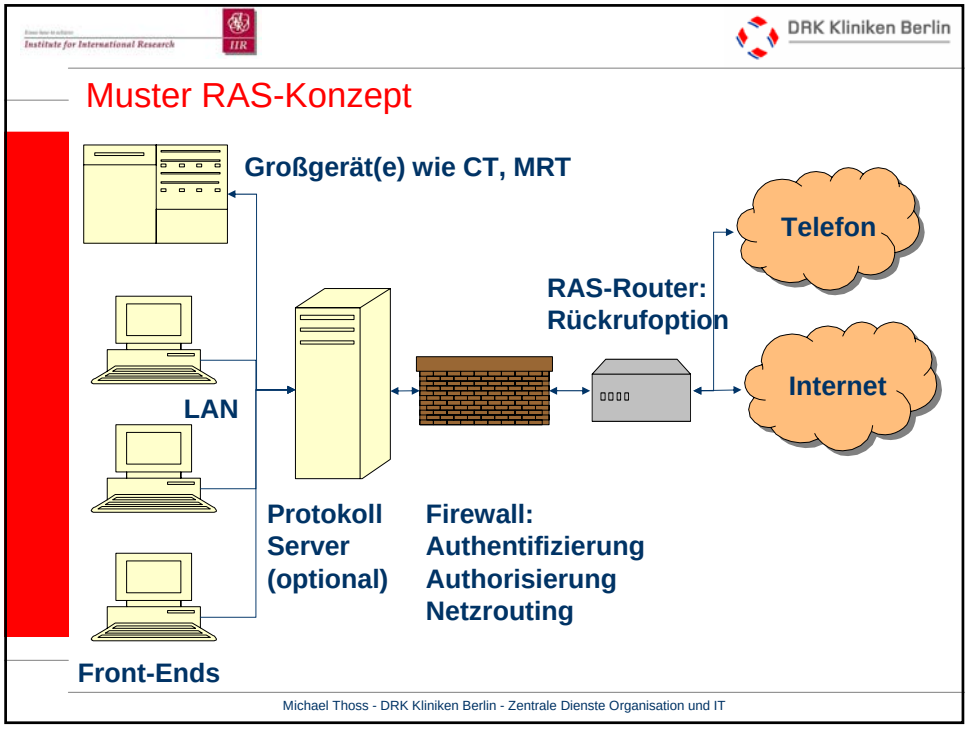

Institute for International Research
IIR
DRK Kliniken Berlin
Muster Internetkonzept (Präsenz)
LAN
Internetpräsenz (gehostet)
Internet
Proxy /
Scanner
Firewall
Router
Front-Ends
Michael Thoss - DRK Kliniken Berlin - Zentrale Dienste Organisation und IT

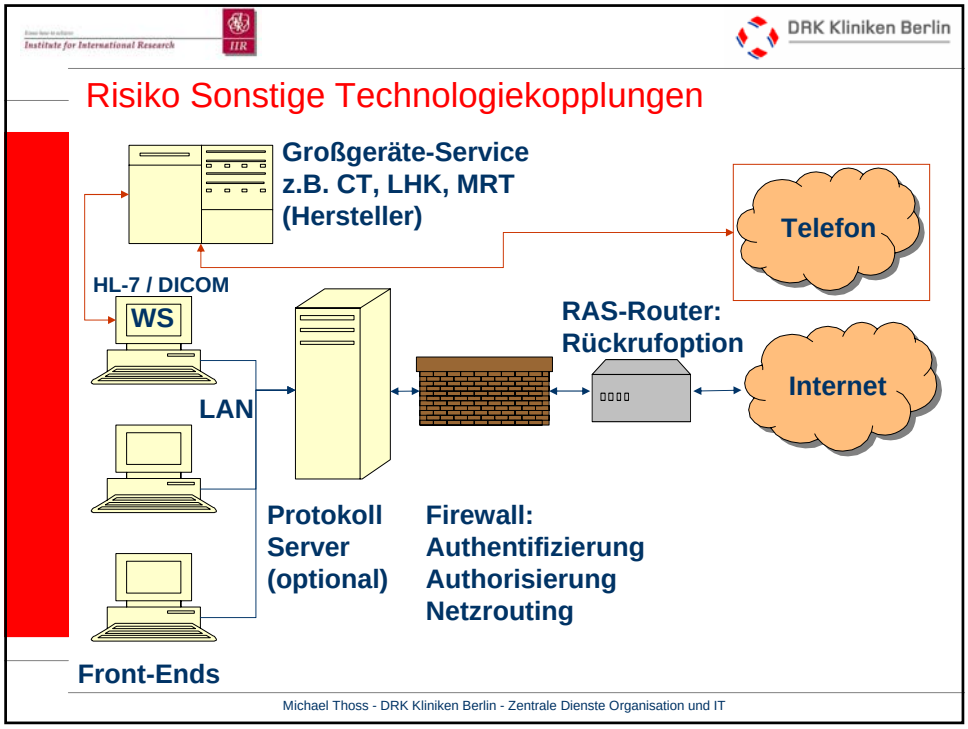
Muster Internetkonzept (Portale)



Muster eMail-Konzept




Institute for International Research
DRK Kliniken Berlin
Muster RAS-Konzept
Großgerät(e) wie CT, MRT
Telefon
RAS-Router:
Rückrufoption
Internet
LAN
Protokoll
Server
(optional)
Firewall:
Authentifizierung
Authorisierung
Netzrouting
Front-Ends
Michael Thoss - DRK Kliniken Berlin - Zentrale Dienste Organisation und IT


Institute for International Research
DRK Kliniken Berlin
Risiko Sonstige Technologiekopplungen
Großgeräte-Service
z.B. CT, LHK, MRT
(Hersteller)
Telefon
HL-7 / DICOM
WS
RAS-Router:
Rückrufoption
Internet
LAN
Protokoll
Server
(optional)
Firewall:
Authentifizierung
Authorisierung
Netzrouting
Front-Ends
Michael Thoss - DRK Kliniken Berlin - Zentrale Dienste Organisation und IT

Die großen ABERs.....:

- Datensicherungen sind auch Sicherheits-architekturen:
- Überproportional viele Datenverlusten resultieren aus nicht geprüften Datensicherungen:

  Fehlerhaftes Beschreiben der Medien
  Fehlerhafte Medien (kein regelmässiger Austausch)
  Keine Recovery-Tests
  Keine Recovery-Szenarien (Betriebshandbuch)

Systemverfügbarkeit ist eine Sicherheit
(wenn auch eine relative...)

- Probleme durchgehender Verfügbarkeiten (Server):
  Hardware
  Betriebssystem
  Datenbank
  Applikation
  aber...
  Netzwerk, Anmeldungsserver, PC, Printserver...
- Optionen:
  Hardware: 5*8 bis 7*24 möglich (98,7 – 99,9%)
  Betriebssystem: max. wie HW (tw. Ohne (MS…))
  Datenbank: i.d.R. ohne / wie HW
  Applikation: i.d.R. ohne / wie HW

Gestaltungsschwierigkeiten

- „Verfügbarkeit“ ist immer auf alles bezogen
- Die funktionelle Vielfalt verhindert eine Verfügbarkeit
- Das schwächste (*unwahrscheinlichste*) Glied muss ebenfalls mit 100% abgesichert werden
- Prioritätsabstimmungen notwendig:
  Was ist (wirklich) Priorität 1?
  Unterschiedliche Sichten aus verschiedenen Perspektiven möglich?
  Tatsächliche Ausfallhäufigkeiten?
  Tatsächliche Schadenhöhen?

Das „gelebte“ Datenschutzhandbuch

- Auf Datenschutz verpflichtet wird jeder Mitarbeiter.
  Die Wahrnehmung erfolgt aber oft im Sinne einer „Formalie“.

  Notwendig sind:
- Verpflichtende Regelungen und bindende Verfahren
- Sanktionsoptionen
- Eindeutige Prozesse
- Eventuell Antragswesen für Sonderregelungen (Sensibilisierung via Unterschrift)
- Betriebsvereinbarung (Sanktionsregelung)

Wohin führt das.....?

- Das Betriebshandbuch

Lösung für das Tagesgeschäft
Lösung für die Prozessanalyse
Lösung für Sicherheitsanalysen
Lösung für Szenario-Gestaltung:
a. Erwartete Fälle
b. Unerwartete Fälle (auch das geht!)

z.B. Eskalationswege: Wer benachrichtigt wen bei unvorhergesehenen Zwischenfällen =
→ Keine Redundanzen oder Untätigkeitsphasen in kritischen Situationen
→ Gesteuerte Handlungsverläufe

Organisatorische Voraussetzungen

Wo Sicherheit tatsächlich anfängt…

Geheimnis Organisation

- Technische Lösungen reichen nicht aus:
  Sie erfassen Wirkungen aber (häufig) nicht Ursachen

- Betriebshandbuch / Servicedokumentation
- Datenschutzbeauftragte/r
- Schulungen / Sensibilisierungstraining
- Datenschutzhandbuch / Sollkonzept Datenschutz
- Notfallkonzepte / Ausfallkonzepte / Servicehandbuch
- Verfügbarkeitsdefinitionen
- Datensicherheit

- **Wirkungen** können mit Technologie bearbeitet werden!
  Ursachen nur mit Organisation und Schulung

Datenschutzbeauftragter

- Interne Vergabe:

  Interessenkonflikt
  Weisungsgebundenheit
  Moderatorfunktion
  (bedingt) Abhängig
  Ressourcenproblem (TZ)

  Sachkenntnis notwendig
  ...

- Externe Vergabe:
  (z.B. WP-Unternehmen)

  Kein Interessenkonflikt
  (weitgehend) Weisungsfrei
  Moderatorenfunktion
  Unabhängig
  Instrumentalisierbar
  Neutral
  Spezialisiert
  ...

Datenschutzhandbuch / Sollkonzept Datenschutz

- Grundlage aller Regelungen in Zusammenhang mit Datenschutz und Datensicherheit
- Medium für organisatorische Regelungen und Umsetzungsentscheidungen (auch außerhalb der IT z.B. in Auskunftsfragen, etc.)
- Position der Unternehmensleitung
- Verbindlichkeit bis auf Detailebene möglich
- Grundlage für Investitionsentscheidungen

Betriebshandbuch

- Regelungen für Standard- und Notfallszenarien
- Definition aller Services und deren Basisverfahren
- „How to do“ für seltene Prozesse
- Systemkennungen, Servicezeiten der Hersteller, Ansprechpartner, Hotlinerufnummern, etc.
- Technische Unterlagen
- Konfigurationshinweise
- Backupverfahren
- Prüfverfahren
- weiteres...

Verfügbarkeit

- Sicherheitsstufen sollten grundsätzlich aus Verfügbarkeitsansprüchen abgeleitet werden
- Verfügbarkeit muss definiert werden
- Kennzahlen helfen weiter
  z.B.: Schadenhöhe, Schadenhäufigkeit, Nutzungszeiten, Spitzenlastphasen
- Wirtschaftlicher Mitteleinsatz sollte stets mit Schadenhöhe im Verhältnis zur Schadenhäufigkeit korrespondieren
- Gesamtverfügbarkeiten sind i.d.R. wirtschaftlich schwer vertretbar (wenn überhaupt vereinbar)

Prioritäten und Verfügbarkeiten

- Eine Ableitung der „Henne oder Ei“-Frage:

  Was gibt es zuerst?

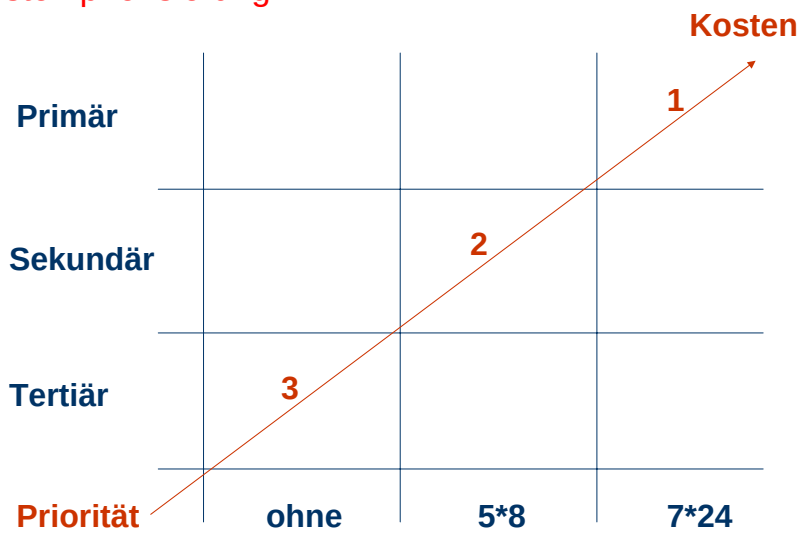
  Das Verlangen nach „Verfügbarkeit“, oder

  die Qualifizierung von „Prioritäten“ (für Systeme)

  In den meisten Fällen: Ruf nach Verfügbarkeit

  Problem:
  Qualifizierung und sachgerechter Mitteleinsatz!

Systempriorisierung



Datensicherheit

- Raumstrukturen (Physikalische Sicherheit)
- Überwachung sensibler Anlagen (physikalisch: z.B. Zugangskontrolle, Temperatur, Brand, Feuchtigkeit, Rauch...)
- Backupverfahren und deren Kontrolle (klassische Backupverfahren (Bänder), Online-Backups)
- Aufbewahrungsfristen
- Zugangs- und Zugriffsverfahren
- Logverwaltung / Kontrollstrukturen
- Sicherheitsarchitekturen für Internet, E-Mail, Netzwerkschutz, Arbeitsplatzschutz, usw.

Aufbewahrungsfristen

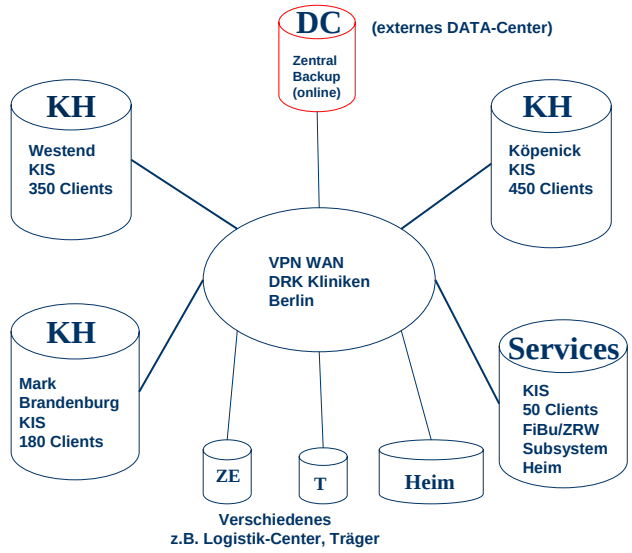
- Betriebswirtschaftliche Daten 7 Jahre
- Röntgenbilder 10 Jahre
- Patientenakten 30 Jahre
- Akten Kinder unter 18 ab 18 bis 48 Jahre
- Röntgenbilder im Rahmen der EPA bis? 30 Jahre

- Anwendungsregelungen:
  ca. 20 gesetzliche Regelungen in der BRD
  Beweiswürdigungsrecht des Richters im Verfahren
  Volumina (Beispiel PACS, moderne Diagnostik)

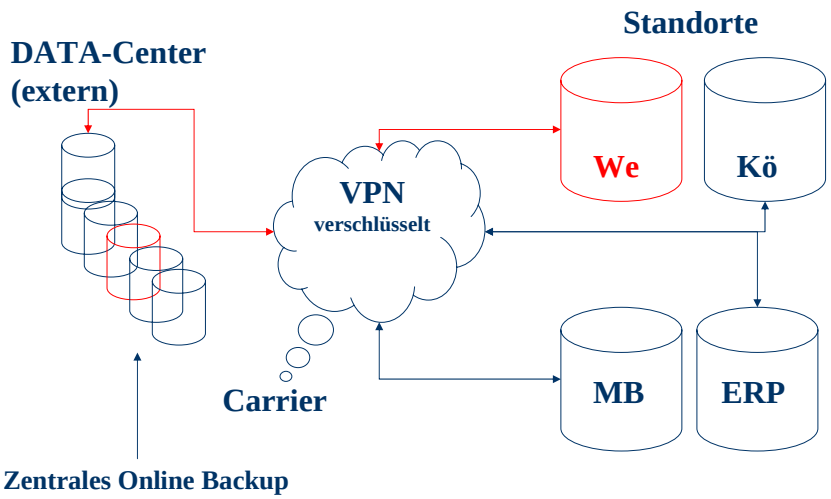
Technisch/Organisatorische Problemstellungen

- Datenvolumen
- Datenmigration aus Technologiewandel (neue Speichermedien, neue Kodierungen, neue Code-Tiefe (8/16/32/64/… bit))
- Medienkontrolle (Verfalldaten, Recovery, Lesekontrollen)
- „Lagerverwaltung“ (z.B. DVDs, …)
- Inventur, Bestandskontrollen
- Absicherung der Verwaltungssysteme (DBs, etc.)
- Lagerorte

EDV-Vernetzung des Unternehmens (Schema)



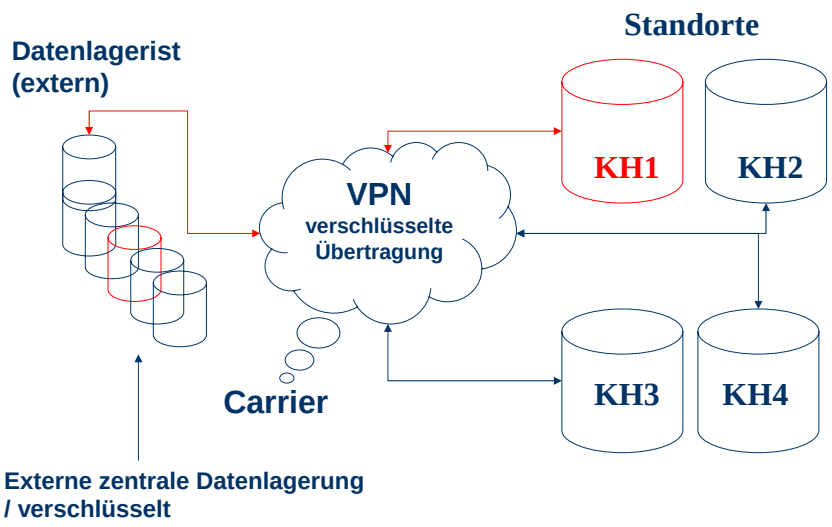
Beispiel: Zentrale Datensicherung KIS



Institute for International Research

DRK Kliniken Berlin

Beispiel: Kernkompetenz Massendatenlagerung?



Institute for International Research

DRK Kliniken Berlin

Sicherheitsprüfungen

Nutzen und Potentiale

Make or Buy

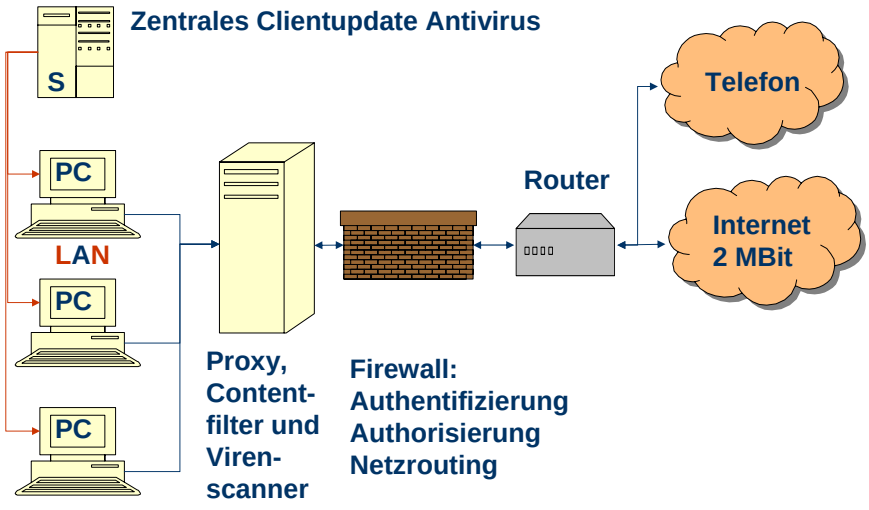
Einrichtungen der
DRK-
Schwesternschaft
Berlin e.V.

Ein Fallbeispiel

- Weitgehende normierte Umgebung:

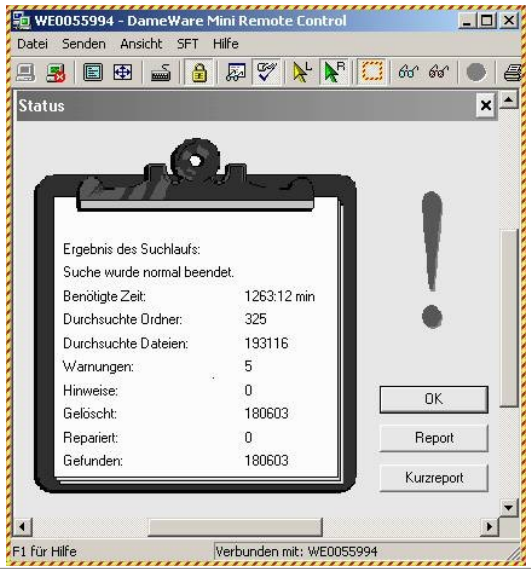
  Zentraler Firewall
  Zentraler Content- und Virenscanner
  Dezentrale Mail-Scanner
  Lokale (PC) Virenscanner
  Automatische Updateverfahren Zentrale Funktionen
  Automatische Updateverfahren lokale Clients
  Relativ wenige offene Wechselmedien (CD, Disk)
  Relativ wenige lokale Admininstratorfunktionen

Muster Mehrstufiges Sicherheitskonzept (vereinfacht)



Von wegen sicher…..

- Dieses Beispiel trat in einer Umgebung ein, die von Administratoren und Leitung als im Prinzip „gut gesichert“ betrachtet ´wurde:



2do: Gefährdungspotentiale ermitteln

- Werkzeug des Qualitätsmanagements
- Schwachstellenanalyse
- Prozessoptimierung
- „Diffamierungs“-Empfindung
- „Betriebsblindheit“-Phänomen
- „Aha!“-Effekte

Qualitätsmanagement und Schwachstellen

- Viele Schwachstellen werden unterschätzt
- Nicht alle notwendigen Prozesse können umgesetzt werden
- Insiderattacken werden von renommierten Beratern für 80% der Schadenereignisse benannt. Das Problem der Wahrnehmung liegt in der Darstellung: „Eine Insiderattacke muss nicht mutwillig erfolgen!“
- Der Fokus der Betrachtung liegt auf externen Bedrohungen (Gründe: Presse, Umgang, etc.)
- Qualitätsmanagement ist schwer messbar zu machen, die Erstellung von Kennzahlen ist mehr als problematisch

„Aha!“ und Prozessoptimierung

- Vorfälle müssen nicht negativ sein, das Risiko ist aber beträchtlich...
- Vorfälle steigern die Aufmerksamkeit aller Beteiligten
- Ein Nutzen muss unmittelbar generiert werden:
  1. Sensibilisierung der Administratoren
  2. Mittelbedarf transportieren und bewilligen lassen
  3. Konsequente und zeitnahe Reaktion:
  3a. Prozessanpassung (Arbeit der Administratoren)
  3b. Fehlerquellenbereinigung (Ursache nicht Wirkung bearbeiten)

„Betriebsblindheit ./. Diffamierung“

- These 1:
  Die meisten Administratoren empfinden (auch konstruktive) Kritik an der Arbeit als Diffamierung derselben
- These 2:
  Entwickler und Administratoren arbeiten überwiegend (ausschließlich) mit Fehlerszenarien, die sie sich selbst vorstellen können

Folgen

- Aus These 1:
  Mögliche Konsequenzen denkbarer Fehlerquellen werden unterschätzt oder zu sehr relativiert

  Killerphrasen:
  „Das kann bei uns nicht passieren“
  „Das haben wir schon immer so gemacht“
  „So was ist bei uns noch nie passiert“
- Aus These 2:
  Prüfungen und Testroutinen entsprechen nur der Erwartungshaltung aber nicht den Möglichkeiten

Option 1: Interne Prüfungen

- Sensibilierung (TOYOTA: „Nichts ist unmöglich“)
- Qualifizierung (Ziel: Horizonterweiterung)
- Konsequentes Handeln (Stets)
- „Neue Wege“ (auch Werkzeuge)
- Sachgerechte Ressourceneinteilung und -freistellung (ausgewogenes Zeitmanagement)

Option 2: Externe Prüfungen

- Qualifizierte Standards verfügbar
- Breite Wissensplattform verfügbar
- Ressourcenschonung intern
- Sachgerechtes Szenario schaffen
- Keine Einschränkungen z.B.
  „bekannte schwarze Schafe (Systeme)“
- Phase 1: Zero Knowledge
  Phase 2: Knowledge
- Keine Angst vor Ergebnissen!
- Auch schlechte Ergebnisse verbessern Qualität!

Erkenntnisse nutzen und umsetzen

- **Nicht** relativieren !
  Administratoren neigen zur Ansicht:
  „Das kann uns nicht passieren“
  „Den Server wollten wir schon lange abschalten...“
- **Niemals** „einschlafen“
  Auf Grund von Auslastung und Ressourcenproblemen werden Prozesse nicht konsequent umgesetzt (u.a. wegen Annahme aus 1.)
- **Ständig** prüfen, **nicht** auf Automatiken verlassen!

Weitere Option(en) für externe Unterstützung

- Überprüfung von Raum- und Gebäude bzw. Infrastrukturen durch Fachleute
- „Serverraumsicherheit“
- Mindestausstattungen:
  Brandüberwachungen (Zonenprinzip)
  Wärmeüberwachung (Kühlungsausfall)
  Feuchtigkeitsüberwachung (Wasserschaden)
  Zugangskontrolle
- (Standard-) Konzepte prüfen!
  Ist der „Doppelboden“ die sachgerechte Lösung…
  (Brandüberwachung ergänzend unter dem Boden usw.)
- Ausbauen oder Auslagern…
- Regelwerk und Argumentationshilfe

Administration und Verwaltung (Make or Buy)

Muss Sicherheit Kern-Kompetenz sein?

Service Abstützung

- „Ist Security wirklich zwingend Kernkompetenz?“
- Ressourcenplanung
- Interner Betrieb
- Externe Abstützung
- Verfügbarkeitsphilosophie
- Fachbereich versus andere Instanzen
- Systempriorisierung

„Ist Security wirklich zwingend Kernkompetenz?“

- **Jein**
  (zu mindestens 50%...)
- IT in der Systemintegrationsverantwortung
- Schnittstellen- und Risikobeurteilungskompetenz
- Verantwortung in erster Linie (delegiert)

- **Aber**
  nicht jeden Job muss man zu 100% selber machen
- Qualifizierte Unterstützung sichern
- Zusätzliche Kompetenzen einbeziehen
- Zusätzliche Argumente nutzen

Fallbeispiel: SPAM

- SPAM-Filter. Erstmal eine gute Idee

- Haken und Ösen:
  1. Postgeheimnis
  2. „Datenverluste“ (kein SPAM…)
  3. Vertrauensproblematik (aussortierte beurteilen…)

- Lösungsansätze?

Qualitätsmanagement

Kann IT Qualität belegen?

Das Problem mit der „Wahrnehmung“

- Differenzierung Störung und Service
- Kummulierte Verfügbarkeiten
- Objektivierung von „geht ja dauernd nicht“
- Statistik
- Eskalationsmanagement
- Externe Unterstützung durch Überprüfung von und über Standards:
  Security-Checks (z.B. Infrastruktur)
  Physikalische Sicherheit (z.B. Serverräume)


Institute for International Research
IIR
DRK Kliniken Berlin
Geschafft !
Vielen Dank für Ihre Aufmerksamkeit !
Falls noch wach: Fragen ?
Einrichtungen der
DRK-
Schwesternschaft
Berlin e.V.