

Vorstellung IEC 80001

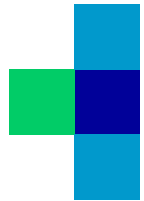
bzw. Erwartungen der Betreiber an die Norm IEC 80001

22.6.2007

Jochen Kaiser

IT-Sicherheitsbeauftragter des Universitätsklinikums Erlangen
jochen.kaiser@uk-erlangen.de

Universitätsklinikum
Erlangen



Seite 2

Vorstellung

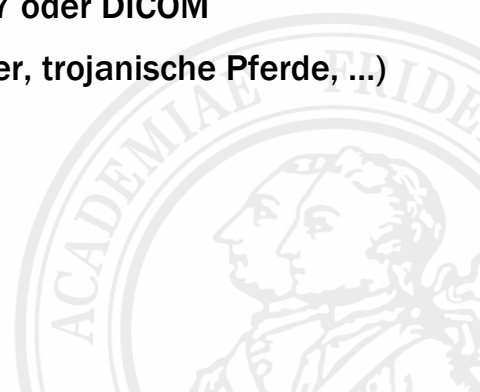
- Jochen Kaiser
- IT-Sicherheitsbeauftragter am Universitätsklinikum Erlangen
- kurze Vorstellung des Universitätsklinikums
- typische Klinik?
 - Vielleicht nicht – aber wir haben alles! 😊



Motivation

- **Vernetzte MP-Komponenten:**
 - **Befundung und Therapie**
 - **Gerätesteuerung und Dokumentation**
 - **Vernetzung von MP Produkten:**
 1. RS232, Bussysteme (USB!), TCP/IP Netzwerke
 2. keine Sicherheitsmechanismen in HL7 oder DICOM
 3. Malware (Internetviren, Internetwürmer, trojanische Pferde, ...)

Jochen Kaiser



Motivation: Problemstellung

- **bisher medizinische und physikalische Risiken**
- **jetzt vermehrt Umgebungsbedingungen beachten:**
 1. andere PEMS (jeweils mit eigener MPG Problematik)
 2. Netzanbindung
(Kupferkabel, Potential, Ableitströme, Kopplung mit Nichtmedizinprodukten)
 3. Einfluss durch interne und externe Netzteilnehmer
 4. Nicht vorhersehbare Aktionen (Netzwerkscan, Multicasting, Anycasting, Verkehrssituation)
 5. (Un-) Verständnis der Netzwerkbetreuung für MPG-Thematik

Jochen Kaiser



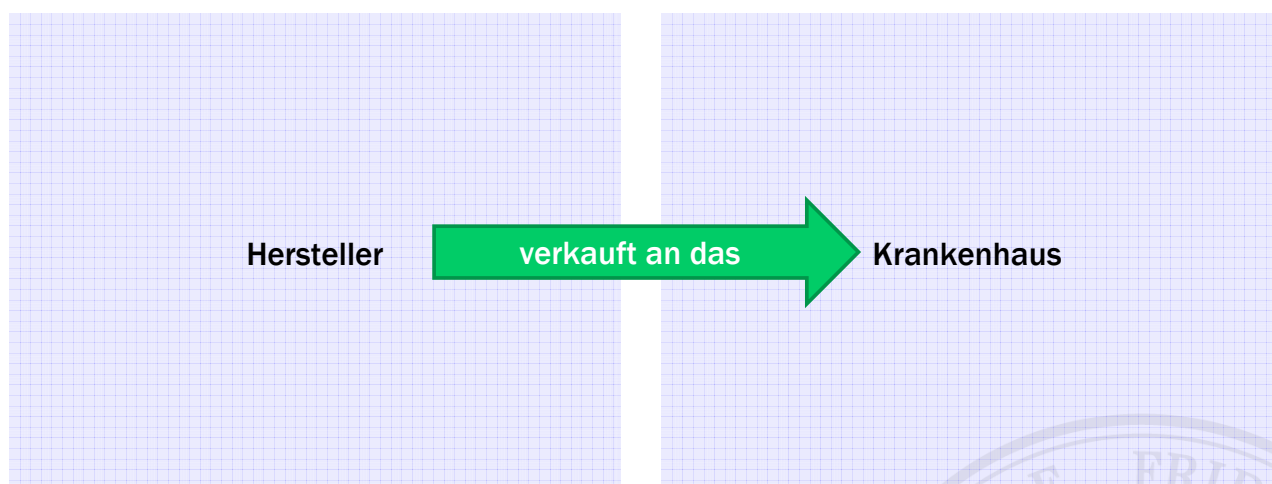
Praxisbeispiele zur Untermauerung

- Infektion von Modalitäten mit Malware
- Kompromittierte Daten
- Systeme werden in Dicom-Verbund gehängt und schreiben Daten in das PACS-System und verursachen dort Probleme
- Systeme stellen Arbeit in großen Netzwerken ein (Broadcastlast zu groß)
- Systeme (Patientenmonitoring & Überwachungsstation) eines Herstellers reservieren gleiche Multicastgruppen (dürfen nur einmal im Netz existieren)
- Hersteller träumt von Microsoft Clusterlösungen ...

Jochen Kaiser



Zuständigkeitsproblematik



Jochen Kaiser

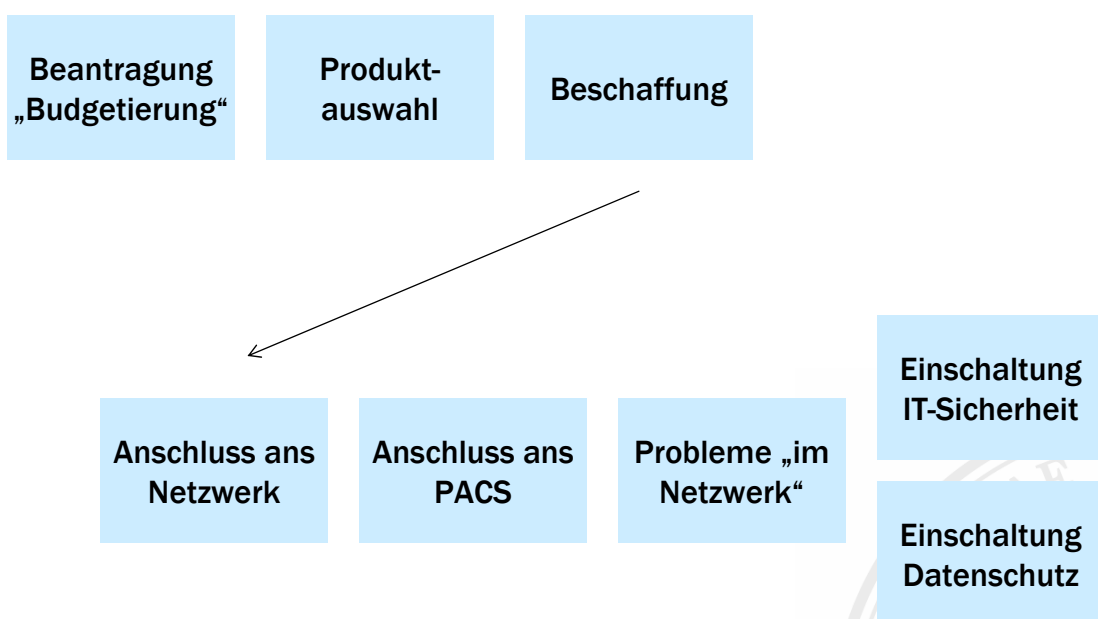


Zuständigkeitsproblematik (Realität)



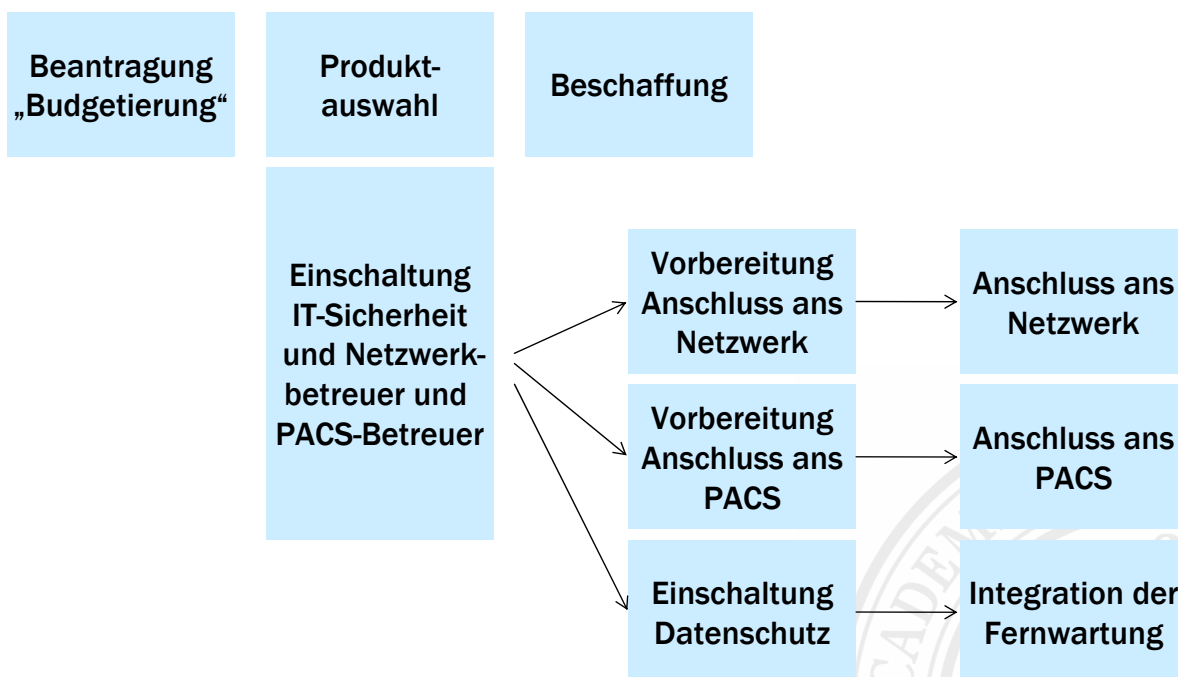
Jochen Kaiser

Realität einer Beschaffung - Lebenszyklus einer Beschaffung



Jochen Kaiser

Gewünschte Abfolge einer Beschaffung - Lebenszyklus einer Beschaffung



Jochen Kaiser

Gesetzeskonformität MPG §30 und §31

- Sicherheitsbeauftragter für Medizinprodukte §30 MPG
- Medizinproduktberater §31 MPG
- IT-Integrator § ??? (keine Regelung!)

- Konsequenz des Autors: Medizinproduktberater und Sicherheitsbeauftragter sind bereits zuständig.
- *Problem: notwendige IT-Kenntnisse für die Beurteilung des Risikos gehören nicht zum Ausbildungsprogramm*

Jochen Kaiser

Vergleich Risiken MT und IT

- **klassische Risiken:**
 - Geräteeigenschaft und Installation
 - Ableitströme, Patientensicherheit
 - Anwendung und Anwender
 - unbekannte Größen: MP, Anwender
- **Neue Risiken:**
 - Netzwerkzugriffe
 - → Vergrößerung der aktiven Komponenten um 4 Zehnerpotenzen
 - Unmenge von Variablen

Jochen Kaiser



Variablen im IT-Datennetzwerk

- **Mit der Vernetzung kommen neue Variablen hinzu:**
 - Eigenschaften des Netzwerks
 - Anzahl der Anschlüsse
 - Topologie, Aufteilung der Segmente
 - QoS-Eigenschaften (Verfügbarkeit, Geschwindigkeit)
 - Ausbildungsstand der Netzwerkoperatoren
 - Sicherheitsmechanismen (Firewall, Virenschutz)
 - Applikation, Prozesse, genutzte Bandbreite

Jochen Kaiser



Maßnahmen zur Verringerung des Risikos

- Genaue Kenntnis über die Eigenschaften des IT-Netzwerks
- Sicherheitsmanagement im IT-Netzwerk
- Kenntnisse über die Eigenschaften des MP
- Kenntnisse über die Eigenschaften des zu koppelnden Geräts
- Fehlerfall Management (Überwachung, Reaktion)
- Übernahme der Umgebungsbedingungen in die Produktentwicklung
- Einsatz eines Systemintegrators

→ **Bedarf an einer Verbesserung der Situation**

Jochen Kaiser

Vorstellung IEC 80001

Pflichten der Hersteller

- Dokumentation der Restrisiken bei Vernetzung

Pflichten der Betreiber

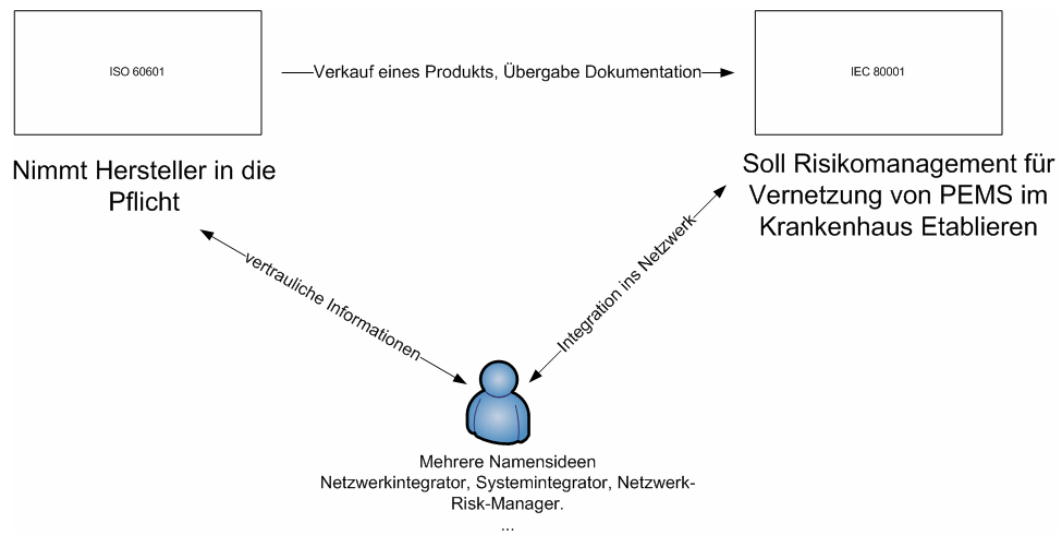
- Dokumentation des Netzwerks
- Übernahme des Restrisikos
- Integration im Netzwerk
- Risikomanagement

(Alles wird schlimmer:

Unter Berücksichtigung der Novelle der 93/42/EWG! Diese definiert künftig „Software“, die zur Diagnose und Therapie eingesetzt wird als MPG.)

Jochen Kaiser

Rolle des Netzwerkintegrators laut IEC 80001



Jochen Kaiser

Eigenschaften des „Netzwerkintegrators“

- Kenntnisse des Netzwerkintegrators
- technologische Kenntnisse:
 1. Medizintechnik
 2. Vernetzung
 3. IT-Sicherheit
- organisatorische Zusammenhänge der Organisation verstehen
- bekommt technische Dokumentation durch den Betreiber
- bewertet das Restrisiko bei Betrieb des Systems im Netzwerk
- erhält Unterlagen zum sicheren Betrieb im Netzwerk
- Unterlagen für Betrieb mit üblichen Sicherheitsanwendungen

Jochen Kaiser

„Gefahren“ der IEC 80001 für Betreiber

- Gefahr 1: Risiken gehen an Betreiber über
- Gefahr 2: Überforderung für kleine Krankenhäuser
- Gefahr 3: Kosten für Integrator
- Gefahr 4: Unkenntnis relevanter Standards

Jochen Kaiser



Forderungen (*nur von mir?*)

- Dokumentation der Probleme nach Lösung der Probleme nicht entbehrlich!
→ es muss weiterhin bei den Herstellern weiterhin an der Lösung von IT-Sicherheitsproblemen gearbeitet werden
- Segmentierung von Netzwerken muss bedacht werden!
- Hersteller müssen Dokumentation über die Risiken und den sicheren Betrieb vorhalten und überlassen:
 1. Verwendung im Kontext einer Firewall: Vorschlag notwendige Konfiguration
 2. Vorschlag Konfiguration Virenschutz
 3. Vorschlag Patchmanagement
 4. Authentifizierungsfragen
 5. Integration in Authentifizierungsstrukturen
 6. technische Meldewege für das MP bei Problemen

Jochen Kaiser



weitere Vorgehensweise

- Krankenhäuser müssen sich koordinieren und den Standard mit gestalten:
 - Standard lesen und verstehen
 - (Treffen)
 - Meinungsbildung
 - Mitarbeit an der Normierung innerhalb der DKE (4-5 Termine/Jahr)

- ein paar Krankenhäuser reden schon miteinander

- Kontaktaufnahme:
 - jochen.kaiser@uk-erlangen.de
 - gerne auch Kontakte zu RK, HELIOS
 - **nächstes Treffen am 5.7.2007 in Frankfurt/M (DKE-Gebäude)**

Jochen Kaiser

