# Elektronische Gesundheitskarte und Gesundheitstelematik

–

# 1984 reloaded?

*Eine unendliche Geschichte*
*Kapitel: Die Sümpfe der Traurigkeit*

Thomas.Maus@alumni.uni-karlsruhe.de

# Überblick

- Einleitung
- Schöne Neue Welt der Gesundheitstelematik
- Realitätscheck zur Schönen Neuen Welt
- Untersuchungsbedarf
- Befunde
- Aut Idem?
- Prognosen
- Antidepressiva
- Fragen und Diskussion

**(Achtung: Forschungsergebnisse + Meinung!)**

# Einleitung

*Was hat das mit Ihnen zu tun?*
Sie sind unmittelbar betroffen:

- die ärztliche Schweigepflicht wird unüberschaubaren technischen Gefahren ausgesetzt
- unüberschaubare Haftungsrisiken für Ärzte
- die Intimsphäre der Patienten wird für Ärzte und Patienten unüberschaubaren technischen Gefahren ausgesetzt

# Einleitung …

*Warum sollten Sie mich ernst nehmen?*

- ein Vierteljahrhundert Erfahrung
  in IT + IT-Sicherheit
- ein gutes Dutzend Jahre Beratungspraxis als
  freier IT-Sicherheits-Analytiker + -Architekt
- Sicherheitsanalyse an Vorprojekt durchgeführt
- von BÄK zum „Chef-Kritiker“ ernannt ;-)
- Kristallisationskeim und Informationsbörse
- Häretiker + unter Beschuß (also richtige Spur) …

# Schöne Neue Welt der Gesundheitstelematik

Ulla Schmidt, Bundesgesundheitsministerin zur Gesundheitskarte (pars pro toto):

- "nachhaltige Revolution im Gesundheitswesen"
- "mehr Qualität, Wirtschaftlichkeit und Transparenz sowie weniger Bürokratie" für Patienten, Ärzten und Kassen

Quelle: Berliner Zeitung, 13.07.2005

# Schöne Neue Welt der Gesundheitstelematik

- Verwendung von „Smart-Cards“ (Signaturkarten)
- Versichertendaten und Bild (obligatorisch)
  - Vermeidung des Versichertenkartenmißbrauchs
  - Stammdatensatz leicht zugänglich
- eRezept (obligatorisch)
  - Vermeidung des Verordnungsmißbrauchs
  - Vermeidung Medienbruch + Mehrfacherfassung
  - → Zeit + Kostenersparnis in Praxis und Apotheke

# Schöne Neue Welt der Gesundheitstelematik …

- Notfalldatensatz
  - Blutgruppe
  - Chronische Erkrankungen, Implantate
  - Allergien + Unverträglichkeiten
  - …
- Verträglichkeits + Wechselwirkungsprüfung
  - eRezept → übergreifende Arzneimittelhistorie
  - Notfalldaten → Allergien + Unverträglichkeiten
  - automatische Prüfung

# Schöne Neue Welt der Gesundheitstelematik …

- eArztbrief
  - schneller elektronischer Austausch von Befunden
  - Beschleunigung der Abläufe
- ePatientenakte
  - komplette Historie der Akte
  - sämtliche Untersuchungsergebnisse

  → Effizienz-, Transparenz- + Qualitätssteigerung (z. B. Vermeidung von Doppeluntersuchungen)

  → medizinische + pharmazeutische Forschung

# Schöne Neue Welt der Gesundheitstelematik …

- Stärkung Patientenposition
  - Dateneinsicht detailliert freigeben + sperren
  - Patient hat volle Einsicht in seine Akte
- Verbesserung IT-Sicherheit Gesundheitswesen

**Schaar:** *Auch heute haben wir ja schon elektronische Systeme in den Praxen, mit denen Patientendaten verarbeitet werden. Diese Systeme sind häufig nicht wirklich sicher. Teilweise ist nicht einmal ein Passwort-Schutz vorhanden, von einer verschlüsselten Speicherung ganz zu schweigen. Auch bei Papierkrankenakten ist der Zugriff Fremder nicht immer ausgeschlossen. Dem gegenüber würde die neue Telematik-Struktur, sofern die gesetzlichen Vorgaben eingehalten werden, auf jeden Fall einen Gewinn bedeuten.* Interview mit **facharzt.de**, 21.09.2005

# Realitäts-Check zur Schönen Neuen Welt

- Darf man so großartige Visionen der Politiker denn überhaupt kritisieren?
- „Wer Visionen hat, sollte zum Arzt gehen.“

(Bundeskanzler Helmut Schmidt)

# Realitäts-Check zur Schönen Neuen Welt

- Technikeinsatz: immer Chancen + Risiken
- Kosten/Nutzen/Risiko-Abwägung notwendig (mehr als nur Technologiefolgenabschätzung)
- Gesundheitskarte + -telematik = ein nicht-existentes System im Wandel … ;-)
- Über was also diskutieren?
- Systematische Betrachtung der gepriesenen Vorteile …

# Realitäts-Check zur Schönen Neuen Welt

- Eignung der Technologien für Einsatzzweck
- Kostenersparnis und Wirtschaftlichkeit
- eRezept
- Notfalldatensatz
- Wechselwirkungs+Verträglichkeitsprüfung
- eArztbrief
- ePatientenakte
- Stärkung Patientenposition
- Verbesserung IT-Sicherheit Gesundheitswesen

# Realitäts-Check
# Eignung Technologien

- E4hoch-evaluierte Chipkarten (intensiv gehärtet+getestet!)
  - Risiko: unsachgemäße Nutzung
    → Sicherheitsanalyse Modellversuch
  - Bedrohung: Bildschirmsicht ≠ Chipkartensicht
  - Tastatur kein sicherer Kanal → PIN ausspähbar
- Theorie? Praxis! – Signtrust Juni 2001
  - Post-Tochter bot Signatur-SW eTrust, BSI-zertifiziert
  - Informatiker (Uni Bonn) griffen obige Schwächen an
  - Meldung an Post, BSI und RegTP im Februar 2001
  - Kritiker erst ignoriert, dann abgestraft ...

  → Mai 2002: Schließg? Signtrust defizitär fortgeführt ...
- Desinfektion Chipkarten, Leser, Tastaturen?

# Realitäts-Check Kostenersparnis+Wirtschaftlichkeit

- Offizielle Zahlen (z.B. Handelsblatt 15.4.05)
  - 80.000.000 Versicherte
  - 180.000 Praxen von Ärzten + Zahnärzten
  - 21.000 Apotheken
  - 2.200 Krankenhäuser
  - 260 Krankenkassen

# Realitäts-Check ... Kostenersparnis+Wirtschaftlichkeit

- Offizielle Kosten/Nutzen-Analyse fehlt (1.11.05)
  - seit mehr als 6 Monaten von KBV beauftragt …
- noch keine Ausschreibung → keine Angebote
  - Kosten also unbekannt
  - Riesenprojekt → kleiner Bieterkreis
  - politische Festlegg → schwache Verhandlgsposition → Bieter-Markt → hohe Kostenrisiken
- Schätzungen der Einsparungen
  - Ersparnis 1 G€/a (Schätzung BGMS, Ulla Schmidt)
  - Ersparnis 515 M€/a (1998 Roland Berger & P., 2004 BITKOM)
  - Ersparnis etwa 200 M€/a (aktuelle KV-Schätzungen)

# Realitäts-Check ... Kostenersparnis+Wirtschaftlichkeit

- z.B. Erstinvestitionskosten je Praxis
  - 1.500 € laut KBV
  - 3.500 € laut Dr. Heinz Fanderl, IBM, Modell in Trier
  - 6.045 € laut Kalkulationsvorlage bit4health
    (aktuelle Ausstattg. vorausgesetzt = 60% der Praxen)
    + 745 €/a Betriebskosten (z.B. PC-Wartung fehlt!)
  - eher 10.000 € laut LÄK Sachsen
- Ersatzinvestitionen etwa alle 5 Jahre
  - für alle Teilnehmer
  - insbesondere Austausch der Karten!

# Realitäts-Check ... Kostenersparnis+Wirtschaftlichkeit

- berechnet mittels Kalkulationsvorlage bit4health-Rahmenarchitektur und öffentl. Angaben
- bundesweite Einführung:
  - 2 Mrd. € Erst-Investitionskosten
  - 1,4 Mrd. €/a jährliche Betriebskosten
  - 0,5 Mrd. €/a optimistischstes jährl. Einsparpotential
  - Ersatzinvestitionen alle 5 Jahre

→keinesfalls wirtschaftlich!!!

→Break-Even frühestens ab 2 Mrd. €/a Einsparung!

# Realitäts-Check ... Kostenersparnis+Wirtschaftlichkeit

- Kalkulationsvorlage realistisch???
  - wichtige Posten fehlen, z.B.:
    Gebäude, PC-Wartg, Firewalls + FW-Wartung,
    Hochverfügbarkeitsmaßnahmen,
    RZ-Sicherheitsmaßnahmen/personal ...
- Patientenkarte:
  - laut Kalkulationsvorlage 10 €/Karte
  - laut Herstellern 15-20 €/Karte (Ärztezeitung 28.9.04)
- Erstinvestition Krankenhäuser
  - laut Kalkulationsvorlage 140.000 €/2 Krankenhäuser
  - Modellversuch Trier: 450.000 €/2 Krankenhäuser
    (als Investitionskostenzuschuß des Landes RLP!)

# Realitäts-Check ... Kostenersparnis+Wirtschaftlichkeit

- Wohl unwirtschaftlich + erhebliche Kostenrisiken
  - vorige Folie: >3,2 Mrd. € Erstinstallation!!!
  - Financial Times D.: 3,4 Mrd. € Erstinstallation
  - Kassenzahnärztlichen Bundesvereinigung + Bundesverband der privaten Krankenversicherung: Erstinstallation > 4 Mrd. € (facharzt.de 11.+12.12.2005)
  - Berliner Zeitung, 13.07.2005:
    - lt. Experten bis zu 5 Mrd. € Erstinstallation
    - Zitat Dr. Günter Braun, Siemens: „*Goldgräberstimmung*“

→wesentlich größere Einsparungen erforderlich!

# Realitäts-Check ... Kostenersparnis+Wirtschaftlichkeit

- „schlafende“ Signatur (+ Gelddruckmaschine ;-)
  - „höhere“ Funktionen erfordern „geweckte“ Signatur (ePatientenakte + Zugriffspflege!)
  - „pay per use“ 70 ¢ *oder* Signatur-Flatrate ≈ 80 €/a
    → 6,4 Mrd. €/a für Trustcenter (u. a. **Signtrust** ;-)
  - Betriebskosten? Nein: „private Kosten“ der Bürger!
- Aha! – Meldung in www.faz.net 30.11.2005:
  „Die Postbank kündigte an, ihr Online-Banking mittelfristig auf die sogenannte digitale Signatur umstellen zu wollen ... *Die Karte solle zunächst als Gesundheitskarte getestet werden, danach könne man sie auch für das Online-Banking verwenden ...*“

# Realitäts-Check ... Kostenersparnis+Wirtschaftlichkeit

- *„Das Ganze ist ein Wirtschaftsförderungspro-gramm zu Gunsten der IT-Industrie, das mit Geldern aus dem Gesundheitswesen finanziert wird."*

kritische Anmerkung von *Dr. Janusz Rat*

Vertreter der KZV in der Gematik und Vorsitzender KZV Bayern
(facharzt.de, 12.12.2005)

# Realitäts-Check ... Kostenersparnis+Wirtschaftlichkeit

- Irgendwo mehr Nutzen + Einsparungen in Sicht?
  - eArztbrief + ePatientenakte (freiwillige Anwendg.)
  - offiziell frühestens 2012 ...
  - warum nur ... ;-)

- Qualitätsverbesserungen als Investitionsgrund?

- Detaillierter Blick auf die gepriesenen Vorteile …

# Realitäts-Check
# eRezept

- Handhabungsaufwände: Dr. Heinz Fanderl, IBM
  - 30 s Verbindungsaufbau,10-15 s Authentisierung
  - was ist mit Signieren? (22. NAI, Dez. .2004)
  - was ist mit Handhabung und PIN Patientkarte?
  - je Rezept oder je Position?
  - Patient + Arzt müssen anwesend sein!?
- Erfahrungswerte:
  - e-Card Austria: 30-60 min/d je Arzt (nur Abrechng!)
  - Medica: 70s/Rezept á 3 Verordng (≈ 100/d je Praxis)
- Wie merkt sich der Apotheker eigentlich viele Medikamente bis zu den Lagerschränken???

# Realitäts-Check ...
# eRezept

- Rezepteinlösung im Ausland?
  (eGK deutsche Insellösung, pardon, Exportschlager)
- Rezepteinlösung durch Nachbarn+Pflegedienst
  - eGK des Patienten erforderlich
  - Hausbesuch? Notfall?
- Prüfung durch den Patienten
  - Papierrezept für die meisten transparent und prüfbar
  - ebenso Aushändigung durch Apotheke
  - bei eRezept ebenso?
- Verringerung Mißbrauchspotential???

# Realitäts-Check ...
# eRezept

- die Rettung:
  bit4health-Rahmenarchitektur
  Dokument Sicherheitsanforderungen
  - Seite 19, PAS-12: durchgängige nicht-elektronische Ersatzverfahren gefordert
  - Seite 25, organ. Maßnahmen: begleitende Papierdokumentation → parallel Papierrezepte
  - Reduktion des Einsparpotentials???
  - Doppeleinlösung Papier- eRezept???

→ das eRezept reißt‘s wohl nicht raus ...

# Realitäts-Check Notfalldatensatz

- Rechtssicherheit + Nachvollziehbarkeit:
  - dürfen/können Ärzte sich auf Notfalldaten verlassen?
  - Nachweis welche Notfalldaten wann auf eGK?
- Praktikabilität:
  - O-Ton mehrerer Notärzte: wir können Patienten nicht zuerst nach Ausweisen, Kapseln etc. durchsuchen
  - keine oder zwei eGKs? (kommt das Bild nun?)
  - z. B. Busunfall o. ä.: Patienten getrennt von eGKs, blutverschmiert, Identifikation schwierig ...
  - Katastrophe (Hochwasser, Erdbeben, Schneesturm ...)
    - kein Strom
    - eGKs verloren, verschmutzt, beschädigt, ...

# Realitäts-Check Notfalldatensatz

- Datenschutz+Datensicherheit:
  - Zugang Notfalldaten: zwingend ungehindert+off-line
  - Zugangskontrolle maximal mittels HBA (nur in D!)
  - Zugang möglich über gestohlene HBAs oder Werksarzt bei Vorstellungsgespräch
  - Daten durchaus sensibel: Diabetes, Asthma etc. erblich disponiert ...
- Die Rettung: Notfalldatensatz freiwillig ...

→ der Notfalldatensatz reißt‘s wohl nicht raus ...

# Realitäts-Check Wechselwirkung+Verträglichkeit-P.

- Lücken der „Medikamentenhistorie“:
  - Compliance?
    - nimmt der Patient alle Medikamente?
    - in welcher Dosierung? wann?
    - Beipackzettel-konform wegen Nebenwirkungen abgesetzt?
  - Relevante nicht-verschreibungspflichtige Wirkstoffe?
    - Kaffee, Milch, Grapefruits, ...?
    - Vitaminpräparate (z. B. Vitamin K)?
    - rezeptfreie Medikamente?
  - Verschreibungspflichtige Wirkstoffe
    - aus dem Familienfundus
    - aus dem Internet
    - illegale Wirkstoffe

# Realitäts-Check Wechselwirkung+Verträglichkeit-P.

- Befragung und Beratung zwingend notwendig!
- erfolgt sinnvoller bei Verordnung,
  also beim Arzt, statt erst in der Apotheke!
- *Klarstellung:*
  Wechselwirkung+Verträglichkeitsprüfung,
  richtig gemacht, definitiv segensreich!
  Aber reine Medikamentenliste unzureichend:
  echte Historie = Verträglichkeit + Wirksamkeit

→ „Medikamentenliste“ reißt‘s wohl nicht raus ...

# Realitäts-Check
# eArztbrief + ePatientenakte

- Praktikabilität
  - theoret. Reduktion Übermittlungszeit + Porto möglich
  - Rahmenarchitektur + Modellversuche: ISDN
    CTs oder Röntgenbilder? (typ. X-Ray 40 MB ≈ 1,5 h)
  - Patientenkarte (und PIN!?) erforderlich für
    - Einsichtnahme in Daten
    - → Arztbriefe + Patientenakte nur mit Patient einsehbar – soll Patient warten oder zweimal kommen?
    - Einpflegen von Daten
    - → Versand Arztbriefe + Pflege Patientenakte nur mit Patient – was ist mit Labordaten + komplexen Auswertungen?
  - Arztbriefe/Entlasspapiere brauchen lange wegen bürokratiebedingter Überlastg → Doppeluntersuchg

# Realitäts-Check
# eArztbrief + ePatientenakte

- Vermeidung von Behandlungsfehlern
  - Meldung auf Website von GOIN (www.goin.info): „Amputation gesunder Lungenflügel wegen Informationsdefiziten, ...“
  - durch ePatientenakte wird alles besser!?
- werden Ärzte nach 36-Stunden-Schicht
  - fehlerfrei ePatientakten pflegen?
  - bessere Entscheidungen anhand umfangreicher ePatientenakten treffen?
- wäre die Umsetzung der EUGH-Entscheidung + EU-Arbeitszeitrichtlinie nicht zielführender?

# Realitäts-Check
# eArztbrief + ePatientenakte

- maximaler Schutzbedarf in allen Dimensionen
  - Vertraulichkeit
  - Echtheit
  - Zurechenbarkeit
  - Rechtsverbindlichkeit
  - Verfügbarkeit
- Sicherheitsanalyse von Modell-Implementierung extrem besorgniserregend ...
- Einführung frühestens 2012?
  → komplette Ersatzinvestition erfolgt ...

→ eArztbrief+ePatientenakte reißen‘s nicht raus ...

# Realitäts-Check
# Stärkung Patientenposition

- eGK = universelle Signaturkarte (Ärzte Zeitung 28.9.2004)
  explizit für Patientenverfügungen!
  - Alte/Demente/Blinde/...: Handhabung?
  - Alte/Demente/Blinde: wie prüfen, was signiert wird?
  - werden wenig technikbegabte Patienten die PINs auseinander halten können?
  - wie wird verhindert, dass Pflegepersonal die PINs bekommt/erzwingt?
  - wie PIN-Mißbrauch durch Stellvertreter verhindern?
  - wie wird Abfangen der PIN an Tastatur verhindert?
  - wie manipulierte Bildschirmanzeigen verhindern?

# Realitäts-Check ...
# Stärkung Patientenposition

- Krank + unter Zeitdruck traue ich mir ***nicht*** zu, alle Gefahren zu erkennen und abzuwehren!
- Wie Bürger schützen vor Daten-Begehrlichkeiten in Zwangslagen: Arbeitssuche, Versicherung?
  - Was machen wir bei „freiwilliger“ Preisgabe?
- Schutz vor Preisgabe der Signier-PIN?
  - Signatur-Karte + PIN = rechtsverbindliche Patientenverfügg.+Testament usw.
  - Irrtum
  - Zwang
  - Schlepp + Nepp (Social Engineering)

# Realitäts-Check ...
# Stärkung Patientenposition

→ „Stärkung Patientenposition“ – ehrlich???

→ „eStärkung“ Patienten? Nein Danke! – ehrlich!!!

Übrigens:

Wenn Bürger als so mündig betrachtet werden, wieso dann eigentlich keine demokratische Projektteilhabe und Volksabstimmung???

→ D-Stärkung Bürger? Ja, bitte!!!

# Realitäts-Check
# Verbesserte IT-Sicherheit

- evtl. Sicherheitsdefizite im IT-Bestand – aber:
  - genau deswegen machen die allermeisten Ärzte ihre Praxis-IT ja auch nicht von Außen zugänglich – weder via Internet, WLANs oder Fernwartung!
- neue Bedrohungsqualität+lage durch Telematik:
  - Massenhafte physische Einbrüche in Arztpraxen langwierige logistische Herkules-Aufgabe
  - Ausnutzen evtl. Sicherheitslücken selbst durch Einzeltäter in kurzer Zeit möglich
  - Telematik hochattraktiv: extrem hohe Wertdichte
    → sehr hohe Risikodichte (analog Kernenergie)
    → hochpotente Angreifer, extreme kriminelle Energie

# Realitäts-Check ...
# Verbesserte IT-Sicherheit

- Wertdichte der Gesundheitstelematik
  - Wert Patientendatensatz >100–150€ (konservativ!)
  - Wert Modellregion (10.000 Patienten) > 1–1,5 M€
  - Wert gesamte BRD > 8–12 Mrd. €
- Erfahrungswerte mit IT-Schutz sensibler Daten
  - „Titan Rain“ plündern vertrauliche Daten aus IT der US-Behörden + -Militärs (und auch der Briten?)
  - 40 Mill. Kreditkartendaten an der Quelle gezapft
  - *... und so weiter und so fort in endlos langen Listen ...*
  - bis in meine Anfänge: ≈ 1980 – ein Programmierer überwies sich Rundungsreste aus Zinsberechnungen

# Realitäts-Check ...
# Verbesserte IT-Sicherheit

- Sicherheitstests (Pen-Tests)
  - keine Erwähnung in offizielle Testplänen des BGMS!
  - Gematik: „bis Hacker verzweifelt Tools einpacken“
  - Design-Analyse bis 100fach effizienter als Pen-Tests!
- „Hacker-Test“ als Sicherheitsfeigenblatt?
  (z. B. http://www.heise.de/newsticker/meldung/66284 *und* .../64466)
  - reiner Labortest → realitätsfern, wenig Aussagekraft
  - vorgeschlagenes Preisgeld 50 k€ – lächerlich!
    so wenig Einsatz bei einem unschlagbaren Blatt?
  - Etat „Akzeptanz-Marketing“ 20 M€ → „Hacker-Test“
  - realitätsnaher „Hacker-Test“ ist Akzeptanz-Marketing
  - allerdings: System-Design hat m. E. Schwächen!

# Realitäts-Check ...
# Mindestanforderungen Hacker-Test

- Glass-Box-Analyse unter Alltagsbedingg.
  - auch + gerade Back-End & Auswertung untersuchen
- Preisgeld ≫ 8–12 M€  (nach Steuern! ;-)
  - Faustregel: 1 von 1000 wird bei Gelegenheit kriminell
  - bei dieser Wertdichte eigentlich viel zu optimistisch
- Alltagsbedingg. mittels Gesundheitsdaten von
  - allen Mitglieder des Bundestages
  - Führungspersonal des Gesundheitsministeriums
  - Führungspersonal der Technologieanbieter
  - ❢ eidesstattliche Versicherung der Vollständigkeit
  - ❢ Möglichkeit des öffentlichen Opt-Out der Kandidaten

# Realitäts-Check ...
# Verbesserte IT-Sicherheit

- Betrachtung der Risiken und Schadenspotentiale
- Schmankerl aus dem offiziellen Dokument *Sicherheitsanforderungen zur Rahmenarchitektur* (www.dimdi.de, Version 1.1)
- keine Schmankerl aus der *Sicherheitsarchitektur:* der Hacker-Test soll doch spannend bleiben ...
- Erfahrungswerte
  - e-card Austria
  - kritische Infrastrukturen + Systeme in Deutschland
  - 21C3-Vortrag: Sicherheitsanalyse eines Modell-projekts zu eArztbrief/ePatientenakte in Deutschland

# Untersuchungsbedürftige Risiken und Nebenwirkungen

*Unbefugter Zugriff auf Patientendaten*

- massive Verletzung der Intimsphäre und der Persönlichkeitsrechte
- Krankheitsdispostionen über Generationen ableitbar → gefährdet Versicherbarkeit des Patienten und seiner Nachkommen
- Interpretation als Schweigepflichtverletzung

→ *Vertraulichkeit der Patientendaten hochsensibel, hochattraktives Angriffsziel für viele*

# Untersuchungsbedürftige Risiken und Nebenwirkungen …

*Manipulation von Patientendaten*

- Verlust von Krankengeschichte
- bei sachkundiger Manipulation Gefahr für Leib und Leben
- Interpretation als Kunstfehler
- Haftung

→ *Integrität der Patientendaten hochsensibel, hochattraktives Angriffsziel für Schwerkriminelle*

# Untersuchungsbedürftige Risiken und Nebenwirkungen …

*Fälschung elektronischer Arztunterschriften*

- erlaubt Zugriff auf Krankenakten
- erlaubt Manipulation von Krankenakten
- erlaubt Rezeptfälschungen + Abrechnungsbetrug
- alles rechtsverbindlich dem Arzt zugerechnet!

→ *elektronische Identität des Arztes hochsensibel, hochattraktives Angriffsziel für viele*

# Untersuchungsbedürftige Risiken und Nebenwirkungen …

*Unbefugter Zugriff auf Praxis+Klinik-IT*

- kann – je nach IT-Sicherheit – alle vorigen Risiken auch dort auslösen
- Sabotage + Lähmung Praxis+Klinikbetrieb
- Beweislage? Haftung?

→ *Sicherheit der Praxis+Klinik-Computersysteme hochsensibel, hochattraktives Angriffsziel*

# Untersuchungsbedürftige Risiken und Nebenwirkungen …

Ähnliche Risiko+Schadpotentialeinschätzungen:

- Thesen der Gesellschaft für Informatik zur Elektronischen Gesundheitskarte:
  - Präsidiumsarbeitskreis „Datenschutz + IT-Sicherheit“ (hochkarätig besetzt!)
- Dr. Thilo Weichert:
  - Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein
  - Datenschutz & Datensicherheit 28 (2004) 7 p.391ff
  - Vortrag auf BSI-Tagung 10.-12.5.2005

# bit4health-Rahmenarchitektur Sicherheitsanforderungen ...

- Quelle: www.dimdi.de, Version 1.1
- Verbindliche Basis aller weiteren Entwicklungen!
- Sicherheitsanforderungen
  - 62 Seiten (Kern 32 Seiten) von insgesamt ≈ 1081
  - Ableitung vorrangig aus Gesetzestexten
  - technisch/wissenschaftl. Gesetze nachrangig
  - Qualitätseinschätzg: teils richtig gut, teils weniger ...
  - Lesen! – Bilden Sie sich ein eigenes Urteil!

- Im Original kein Zitieren möglich – bestimmt keine Schikane oder Sicherheitsmaßnahme, sondern nur bedauerliche Panne!
  Abhilfe: pdf2ps *Dokument*.pdf - | ps2pdf - *Arbeitskopie*.pdf

# bit4health-Rahmenarchitektur Sicherheitsanforderungen

- Zitate aus den Sicherheitsanforderungen

**1.1 Ziele des Dokuments**

Ziel des vorliegenden Dokuments ist es, eine Sammlung widerspruchsfreier, gültiger Sicherheitsanforderungen an die Telematik im Gesundheitswesen bereitzustellen.

**2.1 Ansatz und methodische Vorgehensweise**

In diesem Dokument werden die Anforderungen an Datensicherheit und Datenschutz, sowohl an die Telematikinfrastruktur als Basis für die elektronische Gesundheitskarte, als auch an die sicherheitsrelevanten Prozesse zusammengefasst,. ...

...

Die konsolidierten Sicherheitsanforderungen im Text des vorliegenden Dokuments stellen die gesetzlichen Anforderungen, die normativ sind, sowie diejenigen weiterer Quellen, die nicht im Widerspruch zu den gesetzlichen stehen, dar und bilden somit eine Sammlung widerspruchsfreier, gültiger Sicherheitsanforderungen an die Telematik im Gesundheitswesen.

# bit4health-Rahmenarchitektur Sicherheitsanforderungen

- Schutzbedarf + Schutzniveau laut BSI-Grundschutzhandbuch:

| **Schutzbedarf** | **Schadenspotential** | **Schutzniveau** |
|---|---|---|
| niedrig bis mittel | Schadensauswirkungen begrenzt und überschaubar | IT-Grundschutz im Allgemeinen ausreichend und angemessen |
| hoch | Schadensauswirkungen können beträchtlich sein *(z.B. Gefahr f. persönl. Unversehrheit denkbar, Datenmißbrauch erhebl. Auswirkung)* | IT-Grundschutz bildet Basisschutz, ist aber unter Umständen alleine nicht ausreichend. Weitergehende Maßnahmen können auf Basis einer ergänzenden Sicherheitsanalyse ermittelt werden. |
| sehr hoch | Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen *(z.B. Gefahr f. Leib+Leben, Datenmißbrauch katastrophal)* | IT-Grundschutz bildet Basisschutz, reicht aber alleine i. A. nicht aus. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell auf der Grundlage einer ergänzenden Sicherheitsanalyse ermittelt werden. |

# bit4health-Rahmenarchitektur Sicherheitsanforderungen

- Schutzbedarf ...

**5.1 Risikobetrachtung des Informationsaustausches**

Aus der Risikobetrachtung des Informationsaustausches zwischen den Komponenten der Telematikinfrastruktur lassen sich weitere Anforderungen ableiten, die im Folgenden diskutiert werden. Das Zielszenario der elektronischen Gesundheitskarte bedingt einen hohen Vernetzungsgrad

- **von existierenden Primärsystemen[5] und Backendsystemen** - die heute schon sensitive personenbezogene, medizinische Informationen lokal verwalten und speichern.
- **mit hinzukommenden übergreifenden Diensten** - die integrierte und konsolidierte Versicherten- und Patienteninformationen für berechtigte Leistungserbringer bereitstellen.

Durch die Vernetzung und Integration dieser Systeme entstehen neue operative Risiken, die sowohl durch die Erhöhung der Bedrohungen als auch durch die Integration der bisher verteilt und separat gespeicherten Informationen zustande kommen. Dies ist schematisch in Abbildung 2 dargestellt. Für die bisher lokal verarbeiteten Daten (nur beispielhaft dargestellt) wird ein niedriger bis mittlerer Schutzbedarf angenommen (grün), der durch die vorhandenen Maßnahmen und Sicherheitskonzepte abgedeckt ist. ...

- Für Daten in Praxis+Klinik-Computersystemen nur mittleren Schutzbedarf???

# bit4health-Rahmenarchitektur Sicherheitsanforderungen

- Schutzbedarf ...

  Seite 25, oben:

  **Zusammenfassend kann daher der Schutzbedarf der durch die Telematik-prozesse unterstützen Prozessschritte als *hoch* bis *sehr hoch* eingestuft werden,**

- Die Praxis+Klinik-IT nimmt doch an etlichen Prozeßschritten teil?
- Was gilt nun?
- Widerspruchsfreiheit?

# bit4health-Rahmenarchitektur Sicherheitsanforderungen

- ... und Schutzniveau

Seite 34, oben

Zusätzliche Sicherheit kann in dieser Konstellation durch die Verwendung von Intrusion Detection Systemen erreicht werden, die Angriffsversuche frühzeitig erkennen, so dass die Ausnutzung von Schwachstellen frühzeitig unterbunden werden kann. Insbesondere wird damit erreicht, dass die fachlichen Anwendungskomponenten mit Standardmaßnahmen des mittleren Schutzbedarfs (siehe [GSHB]) aufgebaut und betrieben werden können. Ausgenommen sind hiervon die Sicherheitsdienste und zugehörigen Sicherheitsobjekte. Diese sind durch zusätzliche Maßnahmen in dem gesamten Lebenszyklus zu schützen ...

- RAS-6 und RAS-7
- Details in 5.2 und 5.3
- m. E. Schutzbedarf für Primärsysteme zu niedrig angesetzt → Schutzniveau zu niedrig angesetzt!

# bit4health-Rahmenarchitektur Sicherheitsanforderungen

- Richtig gute Sicherheitsanforderungen (m.E.)

| | |
|---|---|
| PAS-12 | **Verfügbarkeit:** Manuelle Ersatzverfahren sind bei Technikausfall für den Prozessschritt vorzusehen. Durch die elektronischen Prozesse sollen bei dem Ausfall einzelner Komponenten keine zusätzlichen Risiken für die Versicherten entstehen. Das derzeitige Niveau muss mindestens erreicht werden. (AS-17)<br>Für jeden neuen und veränderten Geschäftsvorfall soll ein analoger, papierbasierter Prozess existieren. ... |
| PAS-17 | **Authentifizierung und Autorisierung:** Patient muss entscheiden können, wer Daten erhält (Informationshoheit, z.B. auftragsbezogene Zugriffsberechtigungen). (AS-19, AS-37) |
| RAS-4 | Die Sicherheit darf nicht auf dem Vertrauen in einzelne Personen beruhen ... |

...

- Die Anwender im Gesundheitswesen sind gegen ungerechtfertigte Anschuldigungen zu schützen.

# bit4health-Rahmenarchitektur Sicherheitsanforderungen

- Richtig skurile Sicherheitsanforderungen (m.E.)

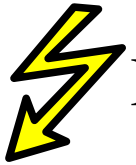
| | |
|---|---|
| MAS-3 | **Flächendeckende Einführung der eGK und der dazugehörenden Applikationen**, um Wirtschaftlichkeit und Durchführbarkeit zu gewährleisten. ... |
| MAS-7 | **Einzug der Karte durch die Krankenkasse**: Bei Beendigung des Versicherungsschutzes oder bei einem Krankenkassenwechsel ist die Krankenversichertenkarte von der bisherigen Krankenkasse einzuziehen (AS-59). |
| MAS-8 | Das Kartenmanagement berücksichtigt eine **mittlere Lebensdauer der eGK von ca. 5 Jahren**. (AS-60) |
| KAS-1 | **eGK:** Die Krankenversichertenkarte (KVK nach § 291 Abs. 1 SGB V/GMG) wird bis spätestens zum 1. Januar 2006 zur Verbesserung von Wirtschaftlichkeit, Qualität und Transparenz der Behandlung zu einer elektronischen Gesundheitskarte (eGK) erweitert. ... |
| KAS-14 | **Optional** wird ein **Abrufverfahren von Daten** (Ticketverfahren) diskutiert. Ggf. flächendeckende Einführung, d.h. ganz od. gar nicht. (AS-47) |

siehe auch Sicherheitsanalyse Modellprojekt ...

# bit4health-Rahmenarchitektur Sicherheitsanforderungen

- Richtig bedenkliche Sicherheitsanforderg. (m.E.)

| | |
|---|---|
| VAS-1 | Eine **Pseudonymisierung des Versicherten- und Leistungserbringerbezugs wird von der Vertrauensstelle durchgeführt** und findet in der Form statt, dass **bundesweit periodenübergreifende Auswertungen zu einem Versicherten und Leistungserbringer durchgeführt werden können**[14]. Pseudonyme enthalten bestimmte Bestandteile (Geburtsdatum, Geschlecht, PLZ, u.a. siehe § 303c SGB V/GMG). ... |



PAS-17

- volle Patientenkontrolle über Datenzugriff???
  - Widerspruch zu öffentl. Versicherungen
  - Widerspruch zu PAS-17, IAS-6, ZAS-1
- Sicherheit der Pseudonymisierung???
  - Geburtsdatum! (selbst Geburtsjahr wäre schon heikel)
    - Raritäten: Babys (Geburt=1. Datensatz!) & 100+-jährige
  - kleine Gemeinden
  - auffällige Krankheitsumstände + Abwesenheiten

# bit4health-Rahmenarchitektur Sicherheitsanforderungen

- Exkurs: die DDR-Personenkennzahl (PKZ)
  „Im Jahre 1969 beschloß der Ministerrat der DDR, eine automatisierte Infrastruktur zur flächendeckenden Kontrolle der DDR-Bevölkerung zu schaffen ... vor allem die Einführung einer Personenkennzahl (PKZ) für alle Bürger und die Errichtung eines zentralen Bevölkerungsregisters. Die PKZ wurde am 1. Januar 1970 eingeführt und mit der Errichtung der Zentralen Personendatenbank Berlin-Biesdorf (ZPDB) 1972 begonnen. Die ZPDB erreichte ihre volle Funktionsfähigkeit knapp zwölf Jahre später, am 1. Januar 1984.“ George Orwell wußte es!
  (http://www.pruefziffernberechnung.de/P/PKZ.shtml)

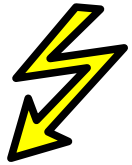
# bit4health-Rahmenarchitektur Sicherheitsanforderungen

- Struktur der DDR-Personenkennzahl (PKZ)
  - Geburtsdatum | $Geschlecht_{Jhd.}$ | Melderegister | lfd.Nr.
- Struktur eGK-Pseudonym = Primärschlüssel!
  - Geburtsdatum | Geschlecht | PLZ | ...
- z.B. Erfurt:
  - früher 11 DDR-Register ↔ heute 12 geograph. PLZ
  - 204.000 Bürger ➔ 17.000 Bürger/PLZ
  - „Pseudonym“-Kollisionswahrscheinlichkeit ≈ 33%
- Welche Daten gibt man Arbeitgebern, Versicherungen + Banken vor Vertragsschluß?
- MetaSTASIerung?

# bit4health-Rahmenarchitektur Sicherheitsanforderungen

- Richtig bedenkliche Sicherheitsanforderg. (m.E.)

| | |
|---|---|
| ZAS-5 | **Unautorisierte Übertragung von Daten(-segmenten) der eGK:** In Ausnahmefällen muss eine Übermittlung von Patientendaten an die GKV sichergestellt werden (Schadensersatzansprüchen gegenüber Dritten). ... |
| PAS-21 | **Authentifizierung und Autorisierung:** Der Schlüssel für die Zusammenführung der Daten ist vom Beauftragten für den Datenschutz des Medizinischen Dienstes aufzubewahren und darf anderen Personen nicht zugänglich gemacht werden. (AS-10) |





- volle Patientenkontrolle über Datenzugriff?
- Nachschlüssel in Obhut einzelner Person?
  - arme Person und Angehörige ...
  - Sparkassendirektoren haben aus gutem Grund keinen unbeschränkt schließenden Tresorschlüssel mehr ...

# bit4health-Rahmenarchitektur Sicherheitsanforderungen

Ich fand keine + vermisse Aussagen zu:

- Schutzziel: Sicherheit der Primärsysteme (Praxis- und Klinik-IT) vor Bedrohungen aus Telematik
- Sicherheitsreserven, etwa:
  - Integritätssicherung durch parallele Verwendung zweier unabhängiger Krypto-Hash-Verfahren
  - Vertraulichkeitssicherung durch parallele Verwendg zweier unabhängiger Verschlüsselg-Verfahren + Schlüssel aus verschiedenen Schlüssel-Generatoren

# bit4health-Rahmenarchitektur Sicherheitsanforderungen

- Beherrschbarkeit der Sicherheit des Systems – Einschätzung der Systemsicherheitsarchitekten:

Seite 28, unten:

**Abbildung 6 zeigt primäre Bedrohungen, die sich auf einen Geschäftsprozess und damit auf konkrete Komponenten (IT-Systeme wie Primärsysteme, Backendsysteme, oder Plattformkomponenten wie Client, Server, Netzwerkkomponenten) beziehen, die den Geschäftsprozess unterstützen. Besteht die Möglichkeit, dass beispielsweise ein Angreifer über ein Primärsystem weitere Komponenten der Telematikinfrastruktur einnehmen kann oder ein Systemfehler einer Komponente zur Korruption anderer Komponenten führt, können auch weitere Geschäftsprozesse durch diese sekundären Bedrohungen betroffen sein. ...**

Seite 29, nach Abbildung 6:

**Wie in obiger Abbildung dargestellt, sind die sekundären Bedrohungen für die Betrachtung des Gesamtrisikos nicht mehr vernachlässigbar: Selbst im Fall einer geringen Eintrittswahrscheinlichkeit für primäre Bedrohungen, so dass ein akzeptables Restrisiko für den direkt betroffenen Geschäftsprozess entsteht, ist die gesamte Schadenshöhe auf Grund der sekundären Bedrohungen nicht mehr zu begrenzen. ...**

# Realitäts-Check ...
# Erfahrungswerte zur IT-Sicherheit

- e-card Austria
- kritische Infrastrukturen+Systeme in Deutschland
- Sicherheitsanalyse eines Modellprojekts zu eArztbrief/ePatientenakte in Deutschland – Vortrag auf dem 21C3

# Realitäts-Check ...
# Erfahrungswerte e-card Austria

- nur Versichertenausweis + Abrechnung (< eGK)!
- Datenschutz
  - Sozialhilfeempfänger erhalten keine e-card
    → Sozialhilfestatus klar erkennbar ...
  - Abrechnungs+Verordnungsdaten des Arztes lassen Rückschlüsse auf Krankengeschichte des Patienten zu
  - Zugriff durch Versicherungen + Arbeitgeber!
    (natürlich nur mit „freiwilliger Zustimmung“ ;-)
- Stabilität und Zuverlässigkeit
  - Totalausfälle: 24.+26.09., 14.12.05, ... (Störfälle? ∞ ;-)
  - laut Hauptverband: „Super-GAUs“
  - Verfügbarkeitsziel: 99,7% (2 RZs)

# Realitäts-Check ...
# Erfahrungswerte e-card Austria

- Risse im Vertrauensfundament
  - Kritik des Österreichischen Rechnungshofes
  - Kostenstruktur selbst *nach* Einführung wohl unklar
  - „Gehaltsskandale“ und „Undurchsichtigkeiten“ bei zentralen Protagonisten
  - Ärzte fordern wenigstens ISO-17799-Zertifizierung
  - e-card-Tagebuch: www.hausaerzteverband.at !!!
- Proteste gegen das System:
  - ARGE Daten
  - Ärztevertretung Östereich/Ärztekammer Wien
  - Österreich. medizin. Softwarehersteller (ÖMS)!!!

# Realitäts-Check ... Erfahrungswerte in Deutschland

- Sowas kann doch in D nicht passieren, oder?
- DMP – Disease-Management-Programme
  - Datenerfassung in Vietnam (bekannt seit Januar 2005)
    - ungeschützter Datentransfer?
    - Verkauf der Daten an „global player“?
    - Staatsanwaltschaft ermittelt ...
  - laut Ärztin (bitte melden, Quelle erwünscht!):
    - Diabetes-DMP-Teilnehmer vom Landratsamt wegen Fahrtüchtigkeit (Visus) angeschrieben worden ...
- Maut-Daten als Fahndungsinstrument
  - Maut-Gesetz explizit mit Zweckbindung der Daten
  - Bundesinnenminister prüft Gesetzesänderung

# Realitäts-Check ... Erfahrungswerte in Deutschland

- Ellis Huber, Ex-Chef Ärztekammer Berlin, jetzt Vorsitzender Securvita BKK
  http://www.aerztlichepraxis.de/artikel?number=1110901029
  "Wenn ein Versicherter mehr kostet als er einbringt, erscheint auf dem Bildschirm des zuständigen Sachbearbeiters ein roter Punkt", so Huber. "Man behandelt ihn dann etwas weniger freundlich." Viele chronisch Kranke müssten demütigende und entwürdigende Auseinandersetzungen mit ihrer Kasse durchmachen. Ein Problem, das laut Securvita-Chef bei allen gesetzlichen Versicherern zu beobachten sei.

# Realitäts-Check ... Erfahrungswerte in Deutschland

- Regionaler Stromausfall August 2004
  - Rheinland-Pfalz (≈ 2/3), Saarland, Luxembourg und Nord-Belgien betroffen, 4–8 Stunden
  - Kaskadenversagen (n+1-Redundanz halt zu wenig ;-)
  - RWE: genaue Ursache nicht feststellbar ...
  - (Mobiltelefone kein taugliches Kriseninstrument ;-)
- Regionaler Stromausfall November 2005
  - Münsterland, teils > 4 Tage
  - Kollabieren von Leitungen unter Schneelast
  - RWE: „höhere Gewalt“ (+ ignorierte Materialprobleme)
- Ausfallende IT-Infrastrukturen? Mal ehrlich ...

# Realitäts-Check ... Erfahrungswerte in Deutschland

- Signtrust (BSI-zertifizierte SW „eTrust“ gehackt)
- BSI verteilt Sober.L auf CERT-Mailing-Liste
- Leuchttürme der Public-Private-Partnerships, Meisterstücke deutscher Technologiekonzerne, Innovationsinitiativen und Exportschlager
  - ALG II Software
  - Toll-Collect
  - InPol Neu (≠ InPol Neu II ;-)
  - Herkules, FISCUS, ELSTER, ...
- Sicherheitsanalyse eines Modellprojekts zu eArztbrief/ePatientenakte ... (→ 21C3)

# Atmosphärische Impressionen ...

- Quelle: Philipp Graetzel Hauptstadtgeflüster 6.11 http://blog.doccheck.com
- bisher der einzige Journalist, der ein Gespräch ablehnte!
- insofern sind die Angaben zu Namen auch nicht von mir.
- Auskunft des Kunden: auch nicht von uns
- welche Quellen?

**06.11: Über die Langlebigkeit von Halbwahrheiten**

... bereits im Januar 2005 ... in der Zeitschrift eHealth inside/der gelbe dienst ...:

„Totalschaden“, „riesige Datenschutzlücken“, „Bastler ohne Praxis“ – was verbirgt sich wirklich hinter einem zum Jahreswechsel entdeckten Datenschutz-GAU bei der elektronischen Gesundheitskarte? Hintergrund: Auf einem Computerkongress in Berlin wurde vage ein Gutachten zitiert, das ein nicht näher spezifiertes IT-Modul der Fraunhofer-Gesellschaft wegen Datenschutzmängeln in der Luft zerreißt. Recherchen zeigen: Das Gutachten wurde von der Kölner Firma MEDNET in Auftrag gegeben, die sich mit der tief in der eGK-Entwicklung steckenden Fraunhofer Gesellschaft vor dem Landgericht Köln zofft. Das Fraunhofer IBMT hat früher mit MEDNET kooperiert und der Firma vor Jahren eine eHealth-Plattform geliefert, die den Sicherheitsansprüchen nicht genügte. MEDNET möchte selbst ein großer Player auf dem eHealth-Markt werden und baut nach dem Platzen der Fraunhofer-Kooperation auf die T Systems-Plattform eHealth Connect, die in Konkurrenz zu der von der Selbstverwaltung favorisierten Fraunhofer-Plattform D2D steht.

... → nächste Folie

# Atmosphärische Impressionen ...

einige Halbwahrheiten:

- Systemalter
- angebl. Kontaktverbot
  - → Auftragsablehng
  - welche „Insider“?
  - „Hey, *X*, gib‘ mir öffentl. unzugängliche Infos, ich will Dich für *Y* hacken“???
- Herr Graetzel auf Mutmaßg. angewiesen?
- Stille Post?

**06.11: Über die Langlebigkeit von Halbwahrheiten**

... →

Bei dem Rechtsstreit geht es um eine Menge Geld, doch die unmittelbare Relevanz für die elektronische Gesundheitskarte ist gering. Das Corpus delicti ist ein vier Jahre altes System mit Sicherheitsmängeln, das sich von dem jetzt in Entwicklung beziehungsweise Einsatz befindlichen deutlich unterscheidet. Dem Gutachter war es nach Auskunft von Insidern außerdem nicht erlaubt, mit dem zuständigen Fraunhofer-Institut in Kontakt zu treten, wodurch er in einigen zentralen Punkten auf Mutmaßungen angewiesen war. Fazit: Wenn demnächst die Sicherheitsarchitektur veröffentlicht wird, ist eine rigide, unabhängige Prüfung durch Datenschützer und Kryptoanalytiker Pflicht. Den aktuellen Vorwürfen dagegen fehlt das Pulver.

# Atmosphärische Impressionen ...

- Quelle:
  Spiegel 7/2005
- Angaben zu Hersteller + System nicht von mir!
- Dipl.-Phys. Bresser
  (lt. IBMT-Organigramm 2004)
  Abteilgsleiter Medizin-Telematik
- Alternative für runden Tisch?

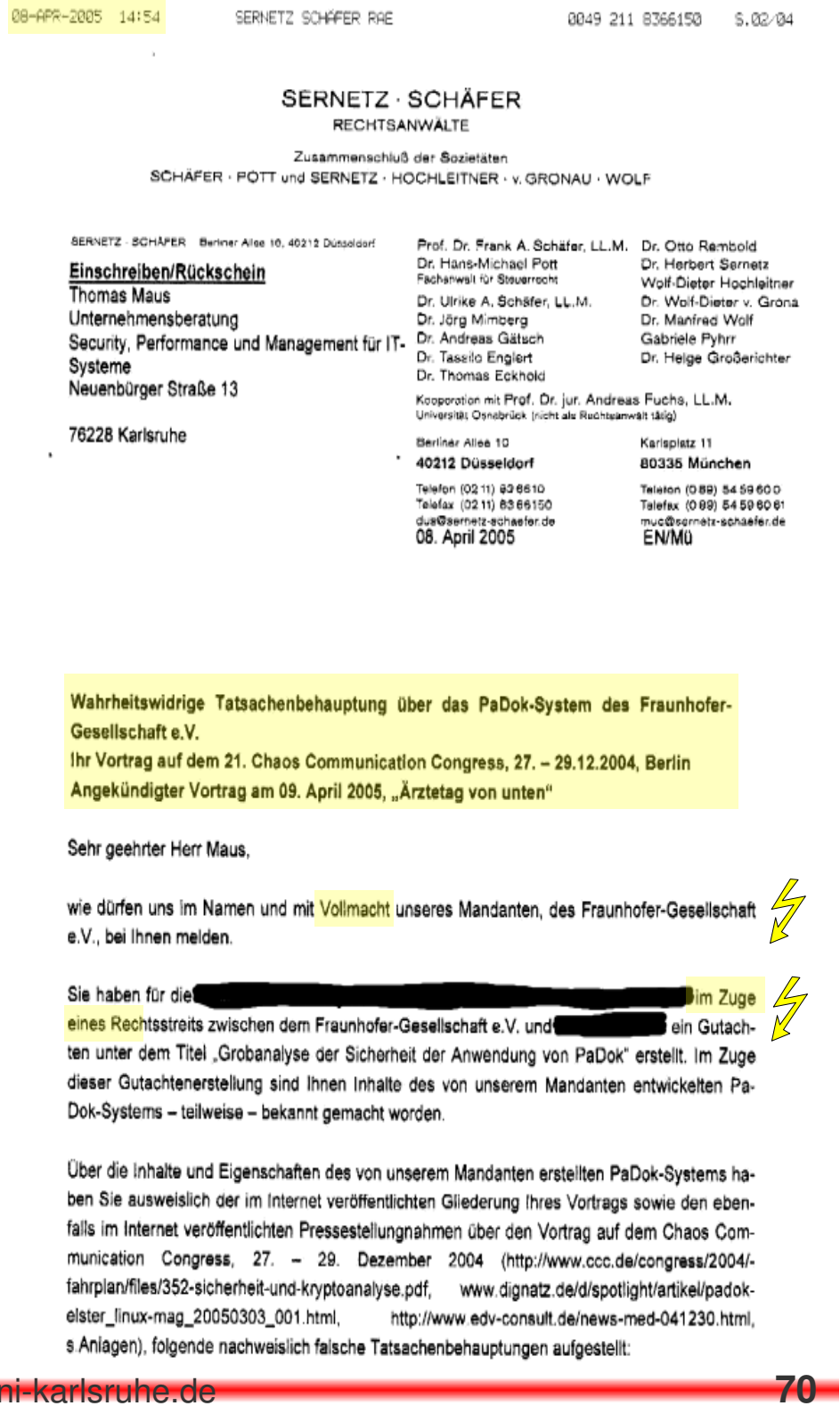
## Wie sicher wird die Gesundheitskarte?

Ein Rechnerverbund zum Austausch von Krankendaten, der bereits in mehreren hundert Arztpraxen und im Rahmen eines Brustkrebs-Projekts im Einsatz ist, soll „eklatante Sicherheitslücken“ aufweisen. Zu diesem Ergebnis kommt der Karlsruher Informatiker Thomas Maus nach der Analyse des Ärztenetzes „D2D/PaDok“. Das Computersystem hat auch gute Chancen, bei der bundesweiten Einführung der elektronischen Gesundheitskarte Modell zu stehen. Dabei hält der Sicherheitsexperte Maus in einem Gutachten fest: „Sowohl Vertraulichkeit, Integrität, authentische Urheberschaft wie auch Verfügbarkeit der Patientendaten sind gefährdet.“ Ihm sei es gelungen, die Kommunikation innerhalb des Systems bis hin zur Schnittstelle für den Kartenleser anzuzapfen. Hackerangriffe gegen „D2D“ seien „von halbwegs talentierten Hobbyisten durchführbar“. Ein Angreifer könnte im Namen eines Arztes Nachrichten signieren und Dokumente fälschen. Bertram Bresser, Mitentwickler von „PaDok“ beim Fraunhofer-Institut für Biomedizinische Technik (IBMT), weist die Vorwürfe zurück: Das „Schlechtachten“ gehe von einem „vollkommen veralteten System“ aus; die Sicherheit sei inzwischen entscheidend verbessert worden.

*Prototyp der Gesundheitskarte*

# Atmosphärische Impressionen ...

- Angekündigter Vortrag
  – 9. April 2005, Berlin
- nebenstehendes Schreiben per Fax am 8.4. ≈ 15 Uhr
- Dipl.-Phys. Bresser, IBMT in Berlin anwesend
- keine Beanstandung ...
- mein Anwalt + ich standen für Klärung vor und außer Gericht zur Verfügung



08-APR-2005 14:54 SERNETZ SCHÄFER RAE 0049 211 8366150 S.02/04

SERNETZ · SCHÄFER
RECHTSANWÄLTE

Zusammenschluß der Sozietäten
SCHÄFER · POTT und SERNETZ · HOCHLEITNER · v. GRONAU · WOLF

SERNETZ · SCHÄFER Berliner Allee 10, 40212 Düsseldorf

**Einschreiben/Rückschein**
Thomas Maus
Unternehmensberatung
Security, Performance und Management für IT-Systeme
Neuenbürger Straße 13

76228 Karlsruhe

Prof. Dr. Frank A. Schäfer, LL.M. — Dr. Otto Rembold
Dr. Hans-Michael Pott, Fachanwalt für Steuerrecht — Dr. Herbert Sernetz
Dr. Ulrike A. Schäfer, LL.M. — Wolf-Dieter Hochleitner
Dr. Jörg Mimberg — Dr. Wolf-Dieter v. Grona
Dr. Andreas Gätsch — Dr. Manfred Wolf
Dr. Tassilo Englert — Gabriele Pyhrr
Dr. Thomas Eckhold — Dr. Helge Großerichter

Kooperation mit Prof. Dr. jur. Andreas Fuchs, LL.M.
Universität Osnabrück (nicht als Rechtsanwalt tätig)

Berliner Allee 10
**40212 Düsseldorf**
Telefon (0211) 83 66 10
Telefax (0211) 83 66 150
dus@sernetz-schaefer.de

Karlsplatz 11
**80335 München**
Telefon (089) 54 59 60 0
Telefax (089) 54 59 60 61
muc@sernetz-schaefer.de

08. April 2005 EN/Mü

**Wahrheitswidrige Tatsachenbehauptung über das PaDok-System des Fraunhofer-Gesellschaft e.V.**
**Ihr Vortrag auf dem 21. Chaos Communication Congress, 27. – 29.12.2004, Berlin**
**Angekündigter Vortrag am 09. April 2005, „Ärztetag von unten"**

Sehr geehrter Herr Maus,

wie dürfen uns im Namen und mit Vollmacht unseres Mandanten, des Fraunhofer-Gesellschaft e.V., bei Ihnen melden.

Sie haben für die [redacted] im Zuge eines Rechtsstreits zwischen dem Fraunhofer-Gesellschaft e.V. und [redacted] ein Gutachten unter dem Titel „Grobanalyse der Sicherheit der Anwendung von PaDok" erstellt. Im Zuge dieser Gutachtenerstellung sind Ihnen Inhalte des von unserem Mandanten entwickelten PaDok-Systems – teilweise – bekannt gemacht worden.

Über die Inhalte und Eigenschaften des von unserem Mandanten erstellten PaDok-Systems haben Sie ausweislich der im Internet veröffentlichten Gliederung Ihres Vortrags sowie den ebenfalls im Internet veröffentlichten Pressestellungnahmen über den Vortrag auf dem Chaos Communication Congress, 27. – 29. Dezember 2004 (http://www.ccc.de/congress/2004/fahrplan/files/352-sicherheit-und-kryptoanalyse.pdf, www.dignatz.de/d/spotlight/artikel/padok-elster_linux-mag_20050303_001.html, http://www.edv-consult.de/news-med-041230.html, s.Anlagen), folgende nachweislich falsche Tatsachenbehauptungen aufgestellt:

- Behauptung "Systemstand 2003" ist falsch. Bestenfalls Stand des Clients, wesentlich ist aber das Gesamtsystem plus Betrieb. Dies wird auch an späterer Stelle konzediert („ältere Systemversion").
- Behauptung: "Unbegrenzter TCP/IP-Verkehr" ist falsch. PaDok benutzt nur einen Port, alle anderen sind zu sperren.
- Behauptung: "Keine Firewall, explizit unnötig" ist falsch. Die derzeitigen Server sind alle mit Firewalls geschützt und auch bei den Clients sind Router mit Firewall empfohlen bzw. vorgeschrieben. Auch bei seinerzeitigem Projekt wurde Firewall und Router bereits empfohlen aber vom Auftraggeber nicht gewünscht.
- Behauptung: "Unbeschränkte TCP/IP-Kommunikationsprofile" ist falsch. Siehe oben.
- Behauptung: "Identitätsstiftende Private-Keys leicht zugänglich" ist falsch. Die Private Keys der Beteiligten können nicht aus deren Karten ausgelesen werden (lt. BSI-Zertifizierung der eingesetzten Telesec-Karten).
- Behauptung: "Alle Private Keys remote zugänglich" ist falsch. Da die private Keys die genutzten Karten nicht verlassen, kann das sachlich nicht stimmen.
- Behauptung: "Angriffsposition A in der richtigen Fachgruppe kann ohne Patientenzustimmung Akte einsehen" ist falsch. Es ist Patiententicket erforderlich.
- Behauptung: "Angriffsposition B besitzt alle Informationen, um Patientenakte direkt und einfach einsehen zu können" ist falsch. S.o. Ticket erforderlich.
- Behauptung: "Patientenschlüssel zeitabhängig + daher leicht vorhersagbar" ist falsch. Zeitabhängig ist lediglich eine Komponente der Ticketbildung einer früheren Version.
- Behauptung: „Bei dem begutachteten System handelt es sich um D2D." falsch. Lediglich eine auf konkrete Kundenforderung angepaßte Version des PaDok-Systems wurde begutachtet.

Diese Tatsachenbehauptungen sind nachweislich falsch. Es besteht daher ein Unterlassungsanspruch unseres Mandanten gegen Sie gemäß den §§ 12, 1004 BGB. Wir weisen Sie nachdrücklich darauf hin, daß aus Ihren wahrheitswidrigen Tatsachenbehauptungen in der Öffentlichkeit eine Schadensersatzpflicht gegenüber unserem Mandanten nach §§ 823, 824, 826 BGB entsteht. Sollten Sie daher bei dem angekündigten Vortrag am 09. April 2005 auf dem „Ärztetag von unten", bei dem potentielle Kunden von unserem Mandanten teilnehmen, erneut wahrheitswidrige Tatsachenbehauptungen über das PaDok-System unseres Mandanten in der Öffentlichkeit aufstellen, kündigt unser Mandant bereits jetzt gerichtliche Schritte gegen Sie an.

Dies vorausgeschickt fordern wir Sie auf, gegenüber dem Fraunhofer-Gesellschaft e.V., z.Hd. Sernetz Schäfer Rechtsanwälte, Berliner Allee 10, 40212 Düsseldorf, sich zu verpflichten, es unter Ausschluß des Fortsetzungszusammenhangs bei Meidung einer für jeden Fall der Zuwiderhandlung fälligen Vertragsstrafe von € 1.000,-- (in Worten: Euro eintausend) zu unterlassen, in der Öffentlichkeit wahrheitswidrig zu behaupten, das von Ihnen untersuchte PaDok-System habe folgende Eigenschaften:





- "Systemstand 2003"
- "Unbegrenzter TCP/IP-Verkehr"
- "Keine Firewall, explizit unnötig"
- "Unbeschränkte TCP/IP-Kommunikationsprofile"
- "Identitätsstiftende Private-Keys leicht zugänglich"
- "Alle Private Keys remote zugänglich"
- "Angriffsposition A in der richtigen Fachgruppe kann ohne Patientenzustimmung Akte einsehen".
- "Angriffsposition B besitzt alle Informationen, um Patientenakte direkt und einfach einsehen zu können".
- "Patientenschlüssel zeitabhängig + daher leicht vorhersagbar".
- "Bei dem begutachteten System handelt es sich um D2D."

Sollten Sie dies nicht ab sofort unterlassen und diese Verpflichtung nicht bis zum

**Donnerstag, den 14. April 2005**

- hier eingehend – dadurch anerkennen, daß Sie die von Ihnen rechtskräftig gegengezeichnete Zweitausfertigung dieses Schreibens an die Unterzeichner zurücksenden, behalten wir uns vor, ohne weitere Ankündigung unverzüglich gerichtliche Hilfe in Anspruch zu nehmen, um die Unterlassungs- und Schadensersatzansprüche durchzusetzen. Zur Fristwahrung reicht die Übersendung per Telefax, vorausgesetzt die Übersendung des Originals folgt unverzüglich danach.

Mit freundlichen Grüßen

Dr. Tassilo Englert
Rechtsanwalt

Hiermit geben Sie die vorstehende Unterlassungs- und Verpflichtungserklärung ab:

_____, den _____ _____

(Unterschrift)

# Atmosphärische Impressionen ...

## Sind FhG, PaDok oder D2D irgendwie relevant für die Gesundheitstelematik?

### TICKET-VERFAHREN IM PRINZIP SEHR GUT

Damit der Zugriff auf in der Telematik-Infrastruktur gespeicherte Daten erfolgen kann, beziehungsweise zur Rechteverwaltung, wird in der vom Fraunhofer-Institut ISST präsentierten Lösungsarchitektur ein Ticket-Verfahren vorgeschlagen. Für ein solches Verfahren spricht der Datenschutz. So fand etwa das im »D2D«-Projekt der Kassenärztlichen Vereinigung Nordrhein verwendete Ticket-Verfahren eindeutige Zustimmung des dortigen Landesdatenschutzbeauftragten. ...

aus der Information Week Special Gesundheitswesen vom 23.6.2005, Seite 34f.

Foto: KBV

HEINZ-THEO REY

**»Ticket-Verfahren sind aus Datenschutz- und Performanz-Gründen zu befürworten; das vom Fraunhofer ISST vorgeschlagene Verfahren ist aber aufwändig und damit potenziell fehleranfällig«.**

**HEINZ-THEO REY,** Leiter der Abteilung IT der Kassenärztlichen Bundesvereinigung

# Atmosphärische Impressionen ... Relevanz FhG, PaDok + D2D

- *facharzt.de:* KV Nordrhein will Test der elektronischen Gesundheitskarte unterstützen
  Die Kassenärztliche Vereinigung (KV) Nordrhein hat dem Gesundheitsministerium des Bundeslandes angeboten, ihre Erfahrungen mit dem Projekt "Doctor to Doctor" für die Testregion der elektronische Gesundheitskarte zur Verfügung zu stellen.

# Atmosphärische Impressionen ... Relevanz FhG, PaDok + D2D

- Überblick Modellregionen + Modelltechnologien:
  http://www.bundesaerztekammer.de/30/eArztausweis/index.html
  - D2D in Heilbronn (BW) + Düren (NRW)
  - Bochum/Essen (NRW) mit D2D?
- FhG IBMT: „PaDok-Verfahren unterstützt elektronischen Gesundheitspass“ (14.11.2005!)
  http://www.innovations-report.de/html/berichte/informationstechnologie/bericht-51632.html
- PaDok/D2D als Prototyp Gesundheitstelematik
  - http://www.heise.de/ct/aktuell/meldung/print/53684
  - http://www.kvbawue.de/kvbw/aktuell/pdf/telem.pdf

# Atmosphärische Impressionen ...

Die verschollene Brille von Zaphod Beeblebrox!

Stuttgarter Zeitung
Nr. 177 vom
3.8.2005

## „Ich bin optimistisch“

### Der Bundesdatenschutzbeauftragte Peter Schaar im Gespräch

*Normalerweise warnt ein Datenschutzbeauftragter, wenn ein System massenweise persönliche Daten verarbeiten soll. Dieses Mal nicht. Peter Schaar freut sich auf die Gesundheitskarte. Warum, hat er Tobias Beck gesagt.*

*Herr Schaar, was ist von der Kritik von Sicherheitsexperten zu halten, die behaupten, dass die Gesundheitskarte im Hinblick auf Patientendaten unsicher wird?*

Ich finde es interessant, dass Kritik schon kommt, obwohl die Karte noch nicht existiert. Wir sind ja nicht mal in der Systemspezifikation so weit, dass wir sagen können: Das ist die Gesundheitskarte. Was wir haben, ist eine ziemlich allgemeine Systembeschreibung. Es ist noch nicht einmal klar, wo und wie die Daten letztlich gespeichert werden.

*Heißt das, die Unkenrufe von Datenschüt-*

*Peter Schaar* Foto Photothek

# Atmosphärische Impressionen ...

- Systemgrobentwurf, der nicht kritisiert, aber gelobt und gepriesen werden kann?
- kritische, fundierte, demokratische Bürger- und Expertenteilhabe etwa unerwünscht?
- Wozu Akzeptanz-Marketing (Budget 20 M€)?
- öffentl. Optimismus (=Akzeptanz) beruht auf
  - Vertrauen in professionelle Skepsis unabhängiger Experten
  - Transparenz
- Wieso direkte Fragen nach meinem Gutachten ignorieren (facharzt.de-Interview)?

# Atmosphärische Impressionen ...

- IT-Kompakt Juni 2005 (BÄK)
- Wunsch Vater des Gedankens?
- Gerichtsbeschluß weder meinem Anwalt noch mir bekannt ...
- Mehrfach Gespräch angeboten ...

## Informatiker Maus abgemahnt

Dem Informatiker Thomas Maus ist mit einer gerichtlichen Abmahnung untersagt worden, nicht wahrheitsgemäße Äußerungen zu dem Fraunhofer-Konzept Padok (Patientenbegleitende Dokumentation) zu tätigen. Maus hatte in den vergangenen Monaten mehrfach über die angeblich gravierenden Sicherheitsmängel eines bestimmten, von ihm untersuchten Systems referiert, dessen Namen er nicht explizit nennen wollte. Nach Meinung des für die Padok-Entwicklung zuständigen Fraunhofer-Instituts für Biomedizinische Technik (IBMT) habe durch die Aussagen von Maus der in den Medien verbreitete Eindruck entstehen können, er spräche über das Padok-Verfahren. Nachdem Thomas Maus zu einem Gespräch nicht bereit gewesen sei, habe die Gesellschaft die Abmahnung gegen ihn erwirkt, um weiteren Mutmaßungen entgegen zu wirken. Das Padok-Verfahren wird unter anderem von der KV Nordrhein unter dem Label „D2D" (Doctor-to-Doctor) für die Übermittlung von Patientendaten zwischen Krankenhäusern und Hausärzten eingesetzt.
www.ibmt.fraunhofer.de

# Atmosphärische Impressionen ...

- Verleiht denn Fraunhofer auch Journalistenpreise?
- Tipp:
  Lesen Sie die Dignatz-Artikel lieber im Original ;-)
- Wunsch Vater des Gedankens?

FhG

Fraunhofer Gesellschaft

Fraunhofer-Gesellschaft Postfach 20 07 33 80007 München

**Einschreiben-Rückschein**

Dignatz Consulting
Herr Eitel Dignatz
Schleissheimer Strasse 87
80797 München

**Recht - B8**

Hansastraße 27c
80686 München

Telefon +49 (0) 89/12 05-0
www.fraunhofer.de

Iris Eigenschenk
Durchwahl +49 (0) 89/12 05-28
Telefax +49 (0) 89/12 05-75 35
iris.eigenschenk@zv.fraunhofer.de

| Ihr Zeichen | Ihre Nachricht vom | **Unser Zeichen** *(bitte stets angeben!)* | München, |
|---|---|---|---|
| | | **B8-4505666** E-ksi | 31. August 2005 |

**Internetveröffentlichungen**

Sehr geehrter Herr Dignatz,

von unserem Institut für Biomedizinische Technik (IBMT) sind wir auf die folgenden von Ihnen im Internet veröffentlichten Artikel aufmerksam gemacht worden:

- Transparenz unerwünscht (http://www.linux-magazin.de/Artikel/ausgabe/2005/04/gastkommentar/gastkommentar.html) und
- Öffentliche IT-Projekte: Transparenz unerwünscht?* (http://www.dignatz.de/d/spotlight/artikel/padok-elster_linux-mag_20050303_001.html)

Die Fraunhofer-Gesellschaft ist die führende Trägerorganisation für Einrichtungen der angewandten Forschung in Europa und betreibt derzeit 58 Forschungseinrichtungen in Standorten in der gesamten Bundesrepublik. Die Institute sind allesamt unselbständige Einrichtungen der Fraunhofer-Gesellschaft und haben keine eigene Rechtspersönlichkeit. Zu den Forschungseinrichtungen gehört auch das IBMT in St. Ingbert.

In den oben genannten Artikel berichten Sie unter anderem über das vom IBMT entwickelte Pa-Dok-System. Sie schreiben:

- "In einem Vortrag hatte der Sicherheitsexperte Thomas Maus über die gravierenden Sicherheitsmängel bei der so genannten elektronischen Patientenakte (Padok, D2D) berichtet."

- "Wer die Details liest, reibt sich verwundert die Augen und fragt sich schließlich, was für Bastler denn dort am Werk waren.....Zum anderen sind die Mängel laut Maus so gravierend, dass er das gesamte Verfahren als nicht reparierbar einstuft."

- "Ein Blick in den Vortragtext zeigt, dass es bei der Verfahrenskonzeption der elektronischen Patientenakte augenscheinlich bereits von Anfang an am kleinen Einmaleins in puncto Sicherheitskompetenz mangelte."

- "Zu klären wäre auch, weshalb das federführend und mit öffentlichen Mitteln alimentierte Fraunhofer-Institut ausgerechnet zu proprietären, nicht offenen Verfahren griff. Es drängt sich der Verdacht auf, dass Intransparenz womöglich ganz bewusst eingesetzt wurde."

Zur Veranschaulichung Ihrer Darstellungen verweisen Sie, sowohl im Textfluss als auch am Ende des Artikels, mittels eines Links auf den angesprochenen Vortrag des Herrn Thomas Maus.

Wir möchten Sie darauf hinweisen, dass zum einen die von Ihnen zitierte Quelle, der Vortrag von Herrn Maus von diesem nach einer Abmahnung unsererseits bereits aus dem Netz genommen wurde und Herr Maus selbst auch Aussagen zum PaDok System wie z.B. dass er die privaten Schlüssel von der eingesetzten Karte ausgelesen hat oder dass das untersuchte System derzeit in Betrieb ist, nicht mehr tätigt und auch nicht mehr veröffentlicht.

Durch die Wahl Ihrer Formulierungen, wie z.B. "...was für Bastler", "...am kleinen Einmaleins in puncto Sicherheit mangelte", "mit öffentlichen Mittel alimentierte Fraunhofer-Institut .....Intransparenz womöglich ganz bewusst eingesetzt wurde " stellen Sie das IBMT und seine Arbeit weiter in einer sehr herabwürdigender Weise dar.

Im oben an zweiter Stelle genannten Artikel schreiben sie weiter:
"Von Einsicht zeigt sich allerdings bis heute keine Spur: Laut Spiegel-Meldung wies Mitentwickler Bresser beim IBMT die Vorwürfe zurück, denn seit dem "Schlechtachten" des Herrn Maus sei die Sicherheit "entscheidend verbessert" worden. Nach dieser Logik wäre es dann auch unfair, die Tschernobyl-Verantwortlichen zu kritisieren: Zum einen bezöge sich eine derartige Kritik auf einen alten Stand der Dinge, außerdem ist weder der Leser noch der Autor dieses Kommentars an den Tschernobyl-Folgen gestorben, und zwischenzeitlich ist die Sicherheit ja schließlich entscheidend verbessert worden, indem man den Sarkophag dicht gemacht hat."

Die hier zitierte Passage, die im Spiegel-Artikel bereits als Verkürzung eines Gesprächs klar erkennbar ist, ist in der vorliegenden Art und Weise der Darstellung extrem missverständlich. Durch das journalistische Mittel der eigenen, direkten Recherche hätten Sie sich ein klareres Bild von der Angelegenheit machen können. Ihr Vergleich zu Tschernobyl ist, unabhängig vom Wahrheitsgehalt der ihm zugrundeliegenden „Informationen" nicht nur unpassend, mit der Sache in keinem Zusammenhang stehend und außerordentlich geschmacklos, sondern trifft allein deshalb schon nicht zu, weil durch den bisherigen Betrieb von PaDok keinerlei Schaden aufgetreten ist.



Wir fordern Sie daher auf,

- auf der Internetseite
http://www.linux-magazin.de/Artikel/ausgabe/2005/04/gastkommentar/gastkommentar.html
den Link zum Vortrag von Herrn Maus zu entfernen,

- auf den Internetseiten
http://www.linux-magazin.de/Artikel/ausgabe/2005/04/gastkommentar/gastkommentar.html
und (http://www.dignatz.de/d/spotlight/artikel/padok-elster_linux-mag_20050303_001.html)
die oben genannte Formulierung, dass Herr Maus das gesamte System als nicht mehr reparierbar einstuft zu entfernen und in Zukunft auch nicht mehr zu verwenden,

- es zu unterlassen, das IBMT und seine Arbeit in herabwürdigender Weise darzustellen,

- den Hinweis auf PaDok/D2D zu entfernen, da auch Herr Maus diese Behauptung nicht mehr aufstellt,

- das oben genannte Spiegel-Zitat von Ihrer Webseite zu entfernen und nicht mehr derartig aus dem Zusammenhang gerissen und missverständlich, ohne Verweis auf den gesamten Artikel darzustellen.

Falls Sie dieser Aufforderung bis zum

**09.09.2005**

nicht nachkommen, behalten wir uns die Einleitung weitere rechtliche Schritte vor.

Mit freundlichen Grüßen

Iris Eigenschenk

Silja Krekel

# Atmosphärische Impressionen ...

- Die Antwort wollte ich Ihnen nicht vorenthalten.
- Macht Appetit ;-)

Schleissheimer Strasse 87
D-80797 München
Tel. 089 - 129 59 97
Fax 089 - 129 59 95
http://www.dignatz.de

**Dignatz Consulting**

Dignatz Consulting, Schleissheimer Strasse 87, D-80797 München

Fraunhofer Gesellschaft
Recht B8
Hansastraße 27c

80686 München

München, den 11.09.2005

**per Fax vorab**

**Ihr Schreiben vom 31.8.2005, AZ B8-4505666**

Sehr geehrte Damen und Herren,

hiermit bedanke ich mich für Ihr Interesse, das Sie meinen Veröffentlichungen entgegengebracht haben.

Die in Ihrem obigen Schreiben gegen mich erhobenen Anschuldigungen sind unsubstantiiert und werden diesseits vollumfänglich zurückgewiesen. Es sei zudem darauf hingewiesen, dass es sich um einen Gastkommentar, mithin also um **Meinung**, handelte, und die Veröffentlichungen dieses Kommentars diesbezüglich unmissverständlich gekennzeichnet sind.

Nach diesseitiger Beurteilung mag es Ihrerseits erwägenswert sein, sich mit der Spruchpraxis zu Art. 5 GG vertraut zu machen.

Den von Ihnen angekündigten rechtlichen Schritten sehe ich mit Interesse entgegen.

Mit freundlichem Gruß

Eitel Dignatz

# Atmosphärische Impressionen ...

- Unterstützung von 2 Organisationen – Danke!
  - Free Software Foundation Europe
  - MEDI-Verband (Ärzte-Organisation)
- MEDI hat sehr umfassend geholfen
- will eigene, unabhängige Begleitstudie zum Modellprojekt Heilbronn finanzieren – Penetrations-Test (aka „Hacker“-Test) inklusive
- wollte ein gutes Verhandlungsklima für sehr sinnvollen Vorschlag – bat daher um etwas „Stillhalten in der breiten Öffentlichkeit“ ...

MEDI Baden-Württemberg

MEDI Baden-Württemberg – Engstlatter Weg 14 – 70567 Stuttgart

Fraunhofer-Gesellschaft zur Förderung
der angewandten Forschung e.V.
Herrn Prof. Dr. Hans-Jörg Bullinger
Postfach 20 07 33
80007 München

2. August 2005

**Sicherheitslücken bei der E-Card**

Sehr geehrter Herr Prof. Bullinger,

mit Schreiben vom 19.07.2005 haben wir Ihnen angeboten, dass Herr Maus nochmals einen von uns finanzierten Angriff auf Ihr Sicherheitssystem bei der E-Card durchführt.

Von unserer Seite besteht ein großes Interesse, dass erstens die Ergebnisse des ersten Angriffs von Herrn Maus und die von ihm aufgedeckten Sicherheitslücken nicht durch juristische Maßnahmen einfach unterdrückt werden. Mindestens so lange nicht, bis nicht der Gegenbeweis angetreten ist.

Außerdem haben wir großes Interesse, dass auch nach Änderung der Sicherheitssysteme diese nochmals von Herrn Maus überprüft werden. Ich glaube, dies ist nicht nur im Interesse der Ärzte, sondern auch im Interesse der betroffenen Patienten.

Könnten Sie mir bitte bis zum 17.08.2005 Ihre Entscheidung mitteilen, damit wir gegebenenfalls gemeinsam mit Ihnen weitere Schritte unternehmen können?

Mit freundlichen Grüßen

W. Baumgärtner

Dr. med. Werner Baumgärtner
Vorstandsvorsitzender

EINGEGANGEN
18. Aug. 2005
Erl.....

Fraunhofer Gesellschaft

Fraunhofer-Gesellschaft Postfach 20 07 33 80007 München

Herrn
Dr. med. Werner Baumgärtner
MEDI Baden-Württemberg
Englstatter Weg 14

70567 Stuttgart

**Der Präsident**

Hansastraße 27c
80686 München

Telefon +49 (0) 89/12 05-0
Telefax +49 (0) 89/12 05-75 00
www.fraunhofer.de

Prof. Dr. Hans-Jörg Bullinger
Durchwahl +49 (0) 89/12 05-10 00
Telefax +49 (0) 89/12 05-77-10 00
hans-joerg.bullinger@zv.fraunhofer.de

München,
11. August 2005

**Ihr Schreiben vom 2. August 2005**

Sehr geehrter Herr Dr. Baumgärtner,

in Ihren Schreiben vom 19. Juli und 2. August bieten Sie uns einen von Ihnen finanzierten Angriff auf das PaDok-System des Fraunhofer IBMT durch Herrn Maus an und weisen auf die Notwendigkeit von Prüfungen der Sicherheitssysteme hin.

Weder lag es, noch liegt es in Zukunft im Interesse der Fraunhofer Gesellschaft Prüfungen, des System zu unterbinden oder juristisch zu bekämpfen. Allerdings behalten wir uns vor, auf die Verbreitung nicht zutreffender Tatsachenbehauptungen zu reagieren. Derzeit gibt es aus unserer Sicht jedoch keinen Anlass, Unregelmäßigkeiten zu verfolgen.

Gerade befindet sich das PaDok-Konsortium in einem Prozess über einen unabhängigen Dritten, zusammen mit der testenden KV, eine BSI-Zertifizierung für "PaDok" zu erreichen. Dazu ist ein neutraler Partner Vorraussetzung, der bereits gefunden ist.

Selbstverständlich steht es Ihnen Herr Dr. Baumgärtner frei, auf eigene Kosten einen solchen Test durchzuführen. Ich würde Sie jedoch bitten, sich in dieser Angelegenheit dann direkt mit dem dafür zuständigen Betreiber, d.h. mit der KV Baden-Württemberg, in Verbindung zu setzen. Die Fraunhofer Gesellschaft wird in diesem Feldtest und in der Geschäftsbeziehung mit der KV selbstverständlich der KV, als der Kundin und Auftraggeberin folgen.

Mit freundlichen Grüßen

Vorstand der Fraunhofer-Gesellschaft
Univ.-Prof. Dr.-Ing. habil. Prof. e.h. Dr. h.c. mult.
Hans-Jörg Bullinger, Präsident

# Befunde
## *Des Kaisers neue Kleider?*

- Gesundheitstelematik birgt neben Chancen erhebliche Risiken (in dieser Ausprägung!)
- Viele Vorteilsversprechen hinterfragungswürdig
- Analyseergebnisse zu früherem Modellversuch mit echten Patientendaten beunruhigend
- Gefahr für Bürger-Gesellschaft und Demokratie
  - Thema nur wenigen Experten zugänglich
  - Kritik nicht nur unerwünscht sondern gefährlich
  - Versuche unabhängige Kritiker auszumerzen

  → Beeinträchtigung der freien Meinungsbildung

# Befunde ...

- Gesundheitstelematik
  *Standardanforderungen an Therapie erfüllt?*
  - Wirtschaftlichkeit – Kosten/Nutzen m. E. ungünstig
  - Angemessenheit – Chancen/Risiko m. E. ungünstig
  - Notwendigkeit – m. E. nicht erkennbar
  - Zumutbarkeit – m. E. weder für Ärzte noch Patienten
  - Wissenschaftlicher Wirksamkeitsnachweis – m. E.:
    - inakzeptable Risiken + Nebenwirkungen sowie Unwirksamkeit nachgewiesen
    - gefährliche Quacksalberei
    - wegen unüberschaubarer Risiken für Ärzte und Patienten Zulassung verweigern ...

# Befunde ...

Angesichts der atmosphärischen Impressionen:
Welchen Mentalitäten können Gesundheitsdaten anvertraut werden, und welchen nicht?

Sind Akteure im Gesundheitswesen denkbar, die ihren Eigennutz über

- die Sicherheit der Patienten stellen?
- die Grundrechte der Bürger stellen?

# Aut Idem?
# Gibt es Alternativen?

- Ich bin Informatiker
  → technophil (aber der Technikrisiken bewußt!)
  → für sichere+innovative Gesundheitswesen-IT die echte Unterstützung leistet
- Versichertenausweis:
  - Lichtbildausweis à la Personalausweis mit maschinenlesbaren Zeichen oder 2D-Barcodes
- eRezept:
  - herkömmliche Papierrezepte mit 2D-Barcodes, elektronisch vom Arzt per HBA signiert

# Aut Idem?
# Gibt es Alternativen?

- Notfalldatensatz:
  - maschinen+menschenlesbare Zeichen auf Versichertenausweis oder separatem Notfallausweis
  - Transponder in Finger- oder Ohr-Ring o.ä.?
  - Implantat??? (Cave! Akzeptanz + Sicherheitsaspekte)
- eArztbrief + ePatientenakte:
  - sogar verschiedene Produkte, beispielsweise
    - Mini-CDs? (EuroMed-ID Systems, Dr. Nehammer)
    - USB-Sticks? (NF-Solutions IT, Hr. Finkernagel)
  - (noch keine Einschätzung meinerseits)
- medizin. + pharmazeut. Forschung:
  - dezentrales Data-Mining (Hr. Kreuscher)

# Prognosen

- Der Worst-Case aus Patientensicht:
  - ein volkswirtschaftliches Desaster
  - dramatische Produktivitäts-, Qualitäts- und Versorgungseinbußen im Gesundheitswesen
  - schwere Betriebsstörungen, insbesondere bei Katastrophen mit besonderem Versorgungsbedarf
  - Zugänglichkeit Patientendaten für bestimmte Kreise
  - resultierend eine 3-Klassen-Gesellschaft: „Weißglas, Grünglas, Braunglas“ + Milchglas
  - wenn die ihre IT-Sicherheit nicht im Griff haben ...
  - „1984“ neben „Heidi“ im Kinderbuchregal

# Für eine bessere Gesundheitstelematik

- Mindestanforderungen für den Hackertest
- Aufklärung der Bevölkerung über die geplante Gesundheitstelematik und Risiko/Kosten/Nutzen

- Mitarbeit an zielführendem System, welches
  - im gesellschaftlichen Konsens ausreichend sicher ist
  - ausreichend Sicherheitsreserven besitzt
  - Schadensbegrenzung + -kompensation a-priori regelt
  - echte Informationshoheit der Bürger gewährleistet
  - barrierefrei – auch hinsichtlich Bildung + Alter – ist
  - nachweislich Nutzen im Gesundheitswesen schafft

# Fragen und Diskussion

*Vielen Dank für Ihre Aufmerksamkeit!*

für Rückfragen
Thomas.Maus@alumni.uni-karlsruhe.de