Gesundheitskarte und Gesundheitstelematik – 1984 reloaded?

Meinungen und Forschungsergebnisse von
Thomas Maus
thomas.maus@alumni.uni-karlsruhe.de

1 Zusammenfassung

Die elektronische Gesundheitskarte steht vor den Türen – ein öffentliches Großprojekt, von dem Gesundheitsministerin Ulla Schmidt sich eine „Revolution im Gesundheitswesen“[1] verspricht. Ungeheures soll die Karte leisten, glaubt man ihren Protagonisten:

- Einsparungen in Milliardenhöhe
- Optimierung der medizinischen Versorgung durch Effizienzsteigerung
- Verbesserung der Versorgungsqualität durch bessere Datenverfügbarkeit
- Stärkung der Patientenposition durch Transparenz und Informationshoheit
- Schaffung von Datengrundlagen für die medizinische Forschung
- und vieles andere mehr ...

Vor dem Hintergrund eigener Untersuchungen an Vorprojekten, dem Studium öffentlich zugänglicher Dokumente und den praktischen Erfahrungen in Österreich glaubt ich – so sehr ich die versprochenen Verbesserungen auch begrüßen würde –, dass die Gesundheitstelematik nach derzeitiger Planung vielleicht doch eher Ungeheuerliches leisten wird:

- Milliardeninvestitionen und -betriebskosten ohne Amortisationschance
- Schwächung der medizinischen Versorgung durch Bindung von Kapital sowie der Kapazität von Fachpersonal
- Verschlechterung der Versorgungsqualität durch Praktikabilitätsprobleme und „erzwungene Hinwendung“ der Mediziner auf den Computer statt zum Menschen
- Schaffung einer hochkritischen, schwer schützbaren Infrastruktur mit extremer Risikodichte
- Auslieferung der Patienten an völlig neue technische Risiken und Abhängigkeiten bis hin zum „Gläsernen Bürger“

Dieser unerhörte Kassandra-Ruf[2] soll im Folgenden begründet werden.

[1] Meine Großmutter pflegte zu sagen: „Bedenke, Kindchen, daß Du bekommen könntest, was Du Dir wünschst!“
[2] siehe auch GUUG FFG 2005 „Das Kassandra-Syndrom“

2 Vorwort

Es sei – zur Ausräumung potentieller Mißverständnisse – vorweg geschickt, dass ich weder Maschinenstürmer noch Gegner einer sinnvollen Nutzung von IT im Gesundheitswesen bin. Ich habe nur als notwendiges Korrektiv zu meiner Technikbegeisterung mein Bewußtsein für die Risiko- und Folgenabschätzung von Technikeinsatz gepflegt – unterstützt aus einem breiten Erfahrungsschatz aus einem Vierteljahrhundert IT-induzierter „Pleiten, Pech und Pannen“ in einer Vielzahl von Einsatzfeldern.

Vor diesem Hintergrund fällt die Analyse der geplanten Gesundheitskarte und Gesundheitstelematik – in aufrichtiger und ernster Sorge um das Wohlergehen von uns allen – weniger euphorisch und weitaus erdenschwerer aus als das offizielle Akzeptanz-Marketing.

Es wäre unverantwortlich, über erkannte Risiken nicht zu reden – Wissen ist Verantwortung.

Und es wäre schön, wenn es einmal gelingen würde, in diesem Lande ein öffentliches IT-Großprojekt durch frühzeitige kritische Begleitung an den Klippen spektakulärer Fehlschläge vorbei zu lenken und so die Akzeptanz, die für den Einsatz der IT absolut unverzichtbar ist, im Gesundheitswesen gerade für die tatsächlich nutzenstiftenden Ansätze des IT-Einsatzes zu erhalten.

3 Schöne Neue Welt der elektronischen Gesundheitskarte

Die Bundesgesundheitsministerin verspricht uns allen – denn praktisch kein Bundesbürger wird sich auf Dauer diesem System entziehen können: eine „nachhaltige Revolution im Gesundheitswesen“ und „mehr Qualität, Wirtschaftlichkeit und Transparenz sowie weniger Bürokratie“ für Patienten, Ärzte und Krankenkassen.

Zwei Pflichtanwendungen soll es auf Basis einer SmartCard geben:

- elektronischer Versichertenausweis – zur schnellen elektronischen Verfügbarkeit der Patientenstammdaten, und zur Eindämmung des Mißbrauch von Versichertenkarten[3]
- eRezept – zur Vermeidung von Medienbrüchen, und damit zur ökonomischeren und schnelleren Abwicklung der Abrechnung, sowie zur Eindämmung des Verordnungsmißbrauchs

Darüber hinaus sind verschiedene freiwillige Anwendungen geplant:

- Notfalldatensatz – zur Verbesserung der Notfallbehandlung sollen freiwillig Blutgruppe, chronische Erkrankungen, Implantante, Allergien und Medikamentenverträglichkeiten gespeichert werden können
- Wechselwirkungs- und Verträglichkeitsprüfung – um Arzeimittelwechselwirkungen, die erhebliches Leid und Behandlungskosten verursachen, zu vermeiden, soll an Hand der Historie der eRezepte automatisch eine Wechselwirkungsprüfung zwischen verschiedenen, parallelen genommenen Medikamenten erfolgen
- eArztbrief – um ärztlicher Kommunikation, wie etwa Entlass-Briefe, Untersuchungsergebnisse, etc. schneller und sicherer als bisher elektronisch auszutauschen
- ePatientenakte – eine Sammlung sämtlicher bisheriger Befunde, der gesamten Krankengeschichte, um Behandlungsfehler durch Informationsdefizite zu vermeiden und Doppeluntersuchungen überflüssig zu machen

Schließlich sollen sich noch weitreichendere systemische Vorteile ergeben:

- durch enorme Einsparungen soll sich das gesamte System binnen kurzen Zeit amortisieren
- die medizinische Forschung soll Zugang zu einer umfangreichen Datenbasis gewinnen
- die Sicherheit medizinischer IT-Systeme soll verbessert werden
- die Patienten sollen volle Kontrolle und Einblick über ihre Daten erhalten

Ein wahres Füllhorn von Vorteilen, Projekt-Amortisierung binnen weniger Jahre – welcher vernünftige und ehrbare Bürger könnte sich ein solch großartigen Vision verschließen!?!

[3] über dessen Ausmaß es übrigens milliardenbreit divergierende Schätzungen gibt, von geringfügig bis gravierend ... Pikanterweise ist meines Wissens bei der damaligen Ablösung des Krankenscheins durch die Speicher-Chipkarten genau vor diesem Risiko gewarnt worden – vergeblich.

4 Erster Realitätscheck

Tatsächlich klingt, wenn sie denn erreichbar wäre, diese Vision absolut gut und unterstützungswürdig – fast zu gut, um wahr zu sein ...

Und so fällt dem neugierigen Bürger als erstes auf, dass trotz der konkreten und detaillierten Anpreisung all dieser Vorteile weder eine solide Kosten-Nutzen-Analyse zu finden[4] ist, noch eine detailierte, implementierungsfähige (oder aus nur ausschreibungsreife), voll spezifizierte Architektur, noch irgendwelche Projekt-, Technologie- oder Sicherheitsrisiken.

Gerade das Fehlen von Risiken, insbesondere im Zusammenhang mit fehlender Detailplanung, widerspricht sowohl dem allgemeinen Erfahrungswissen der IT-ler schon in kleinen, überschaubaren Projekten, als auch der Lebenserfahrung der Bürger bei der bisherigen Einführung neuer Technologien im Allgemeinen und der Durchführung von IT-Großprojekten der öffentlichen Hände im Speziellen.

Bei dem, laut Bundesgesundheitsministerin, größten und anspruchvollsten IT-Projekt im Gesundheitswesen weltweit, welches an vielen Stellen technologisches Neuland betreten soll, kann dies nur ungläubiges Staunen auslösen. Denn natürlich ist mit der Gesundheitskarte alleine noch kein funktionsfähiges System gegeben. Tatsächlich wird, wenn von der Gesundheitskarte geredet wird, meist *pars pro toto* die gesamte Gesundheitstelematik gemeint: ein stark verteiltes, hoch komplexes Computernetz aus hunderttausenden von Systemen.

Ein Realitätscheck scheint daher nicht unangebracht ...

Bevor wir uns also meinem eigentlichen Thema der Sicherheit der Gesundheitstelematik zuwenden, sowie Fragen des Datenschutzes, lohnt ein allgemeiner Blick über das Projekt und die Planungsqualität. Natürlich berühre ich mit diesen medizinischen, juristischen und volkswirtschaftlichen Fragen Gebiete jenseits meiner eigenen Expertise. Ich verlasse mich hier sowohl auf Ihre Kritikfähigkeit wie auch auf das erstaunlich bestätigende Echo von Ärzten, Volkswirten und Juristen ...

4.1 Wirtschaftlichkeit

Die Wirtschaftlichkeit dieses Projektes hängt natürlich vom Verhältnis Kosten/Nutzen ab. Mangels einer öffentlich verfügbaren Kosten/Nutzen-Analyse müssen wir uns selbst Gedanken machen.

Für das Einsparpotential war lange Zeit eine Studie von Roland Berger Strategy Consultant maßgeblich, die Einsparungen in Höhe von 515 Mill. € jährlich prognostiziert. Dem steht eine Studie der Kassenärztlichen Vereinigungen gegenüber, die zu etwa 200 Mill. € jährlich kommt. In jüngster Zeit steigern sich die aus dem Bundesgesundheitsministerium zu vernehmenden Schätzungen für das jährliche Einsparpotential drastisch: Zuerst 1 Mrd. €, inzwischen wohl schon 2 Mrd. € – ein sicheres Indiz, dass das Kosten/Nutzen-Verhältnis dieses Großprojekts noch nicht voll verstanden ist.

Das Bundesgesundheitsministerium gibt die Investitionskosten für diesen Systemkomplex bisher mit etwa 1,4–1,6 Mrd. € an. Dies erstaunt etwas, denn setzt man in die Kalkulationsvorlage für Modellprojekte[5], aus der offiziell verbindlichen bit4health-Rahmenarchitektur (Version 1.1) bei www.dimdi.de, das Mengengerüst des Vollausbaus[6] ein, so erhält man: 2 Mrd. € Erstinvestition und 1,4 Mrd. € jährliche Betriebskosten. Da etwa alle 5 Jahre eine Ersatzinvestition notwendig ist, ergibt sich hier eine Amortisation erst ab etwa 2 Mrd. € jährlicher Einsparungen.

Es gibt aber durchaus gute Gründe, an der Korrektheit der offiziellen Kalkulationsvorlage zu zweifeln. Die Financial Times Deutschland prognostiziert 3,4 Mrd. €, eine Studie der PKVen ergibt 4 Mrd. € und die Berliner Zeitung zitiert Experten mit jenseits der 5 Mrd. € Erstinvestition!

Erfahrungswerte aus einige Vorprojekten zeigen, dass die Kalkulationsvorlage an vielen Stellen zu optimistisch ist. Im Modellprojekt Trier etwa wurde den beiden Modellkrankenhäusern vom Land ein Investitionkostenzuschuß von 450.000 € gewährt. Selbst wenn man etwaige Eigenleistungen

[4] von mir zum Stand 1. Februar 2006 zumindest mit einigermaßen akzeptablem Aufwand unauffindbar
[5] sie ist explizit für die große wie kleine Modellversuche vorgegeben, sollte also die vorgesehenen Mengenstaffeln enthalten, und enthält auch keine Einschränkungen hinsichtlich des Größenbereichs, für den sie gültig sein soll
[6] 80.000.000 Versicherte, 180.000 Arzt+Zahnarzt-Praxen, 21.000 Apotheken, 2.200 Krankenhäuser, 260 Krankenkassen

der Krankenhäuser, und sei es nur Personaleinsatz, ignoriert, liegt dieser Wert weit über den 140.000 €, die die Kalkulationsvorlage für 2 Krankenhäuser ansetzt. Aus dem Modellprojekt Heilbronn sind Zahlen zu hören, die andeuten, dass der Investitionsbedarf in den Arztpraxen ähnlich falsch eingeschätzt wurde. Schließlich sind in der Kalkulationsvorlage die Chipkarten mit je 10 € angesetzt, doch laut Herstellern sind 15-20 € je Karte (Ärztezeitung 28.9.04) notwendig. Setzt man diese drei Erfahrungswerte in die Kalkulationsvorlage ein, so gelangt man zu Erstinvestitionskosten in schwindelerregender Höhe von etwa 7 Mrd. € – etwa das Jahresbudget aller niedergelassenen Fachärzte oder die Administrationsaufwände aller Krankenkassen!

Bei 7 Mrd. € Investition alle 5 Jahre und jährlichen Betriebskosten von 1,4 Mrd. ergäbe sich schon ein Einsparbedarf von etwa 3 Mrd. € jährlich nur zur Amortisation, ohne den Projektrisiken Rechnung zu tragen.

Allerdings fehlen in der Kalkulationsvorlage wichtige Investitions- und Betriebskosten, wie etwa Gebäude, PC-Wartg, Firewalls + FW-Wartung, Hochverfügbarkeitsmaßnahmen, RZ-Sicherheitsmaßnahmen/personal und vieles mehr, das für einen geordneten IT-Betrieb unverzichtbar ist. Somit sind weitere Steigerungen der Schätzungen wahrscheinlich.

Schließlich sind die Ärzte zwingend auf die elektronische Signierfähigkeit der Karten angewiesen und die Patienten benötigen sie, falls sie „höhere" Kartenfunktionen nutzen wollen, insbesondere das Ausüben ihrer Informationshoheit über ihre Daten. Für diese Signaturen werden verschiedene Kosten diskutiert, die von 70 ¢ je Signatur bis zu jährlichen Pauschalen in Höhe von 80 € reichen. Dies würde zusätzliche jährliche Betriebskosten von etwa 6 Mrd. € auf den Schultern der Bürger bedeuten.[7] Eine Amortisation fände dann sogar erst ab etwa 9 Mrd. € jährlicher Einsparung statt und könnte, überspitzt dargestellt, selbst durch kompletten Verzicht auf Krankenkassen oder die fachärztliche Versorgung nicht mehr gegenfinanziert werden.

Durch die strikte politische Vorfestlegung auf ein Großprojekt hat man jedenfalls einen kleinen Bietermarkt geschaffen, der seine eigenen Kostenrisiken birgt. So formulierte etwa Dr. Günter Braun, Siemens, in der Berliner Zeitung: „Die Branche ist in Goldgräberstimmung."

Wenn also kaum vorstellbar ist, dass sich dieses System jemals amortisiert, rechtfertigt dann vielleicht der Gewinn an Qualität, Transparenz oder Kontrolle die Investition?

4.2 Medizinischer Nutzen

Der entscheidende Nutzen wird immer der elektronischen Patientenakte zugesprochen. Konnte man 2004 noch den Eindruck gewinnen, dass praktisch einsatzbereite, erprobte Lösungen bereit stehen, wird zwischenzeitlich an verschiedenen Stellen davon ausgegangen, dass mit deren Einsatz kaum vor 2012 zu rechnen sei.[8]

Die Konzentration soll hier daher auf den Nahzielen liegen: dem eRezept, der Wechselwirkungsprüfung und dem Notfalldatensatz.

4.2.1 eRezept

Das eRezept selbst bietet kaum medizinischen Nutzen – schließlich gibt es kaum noch handgeschriebene, unleserliche Rezepte –, aber durchaus einige Risiken und Praktikabilitätsfragen:

- Bleiben die Verordnungen mit den Versichertendaten oder auch nur der Versichertennummer verknüpft, läßt sich an Hand der Medikation häufig ein sehr präzises Bild über die Diagnosen gewinnen – wir werden im Kapitel „Sicherheit" die weitreichenden Konsequenzen diskutieren.
- Von der Medica 2005 wird berichtet, dass eine Rezeptausstellung rein technisch mit etwa 70 Sekunden Zeitaufwand zu Buche schlägt – dabei sind Verzögerungen durch gehandicapte[9] Patienten noch garnicht berücksichtigt. Bei etwa 100 Rezepten pro Tag in durchschnittlichen Praxen bedeu-

[7] Natürlich könnte sich ein Teil der Bevölkerung dies nicht leisten. Neben der offenkundig resultierenden Zwei-Klassen-Gesellschaft birgt der Verlust der Informationshoheit, wie wir noch sehen können, für diese Menschen, ihre Kinder und Kindeskinder ernste Risiken.

[8] Also letztlich nach einer kompletten Ersatzinvestionsperiode, so dass sich die Frage stellt, warum man nicht einfach wartet, bis das Hauptzugpferd, die ePatientenakte, bereit steht. Ohnehin klingt diese Zeitperiode eher nach einer kompletten Neuentwicklung denn nach Feinschliff nahezu einsatzreifer Modelle, so dass man die Erkenntnisse aus dieser Entwicklung hinsichtlich Machbarkeit und Sicherheit sinnvollerweise abwarten sollte.

[9] Patienten etwa, die mit 40°C Fieber oder anderen beeinträchtigenden Krankheitswirkungen ihre PIN vergessen oder mehrfach falsch eingeben, Demente, stark Sehbehinderte, Zittrige, ...

tet dies etwa 2 Stunden Zusatzaufwand[10]. Zum Quartalsbeginn in einer Landpraxis in der Schnupfensaison fallen aber häufig 300 Rezepte am Vormittag an. Dies entspricht dann einem Zusatzaufwand von 6 Stunden, die der Vormittag einfach nicht hat – eine Situation, die technisch wohl als Systemkollaps zu bezeichnen ist und grundsätzlich die Frage aufwirft, wie so eine zeitnahe, ja sogar verbesserte Versorgung, auch und gerade bei Epidemien, erreicht werden soll.

- Geht der Kranke nicht selbst zur Apotheke, muß er die Gesundheitskarte aus der Hand geben, damit das eRezept auf der Karte eingelöst werden kann. Ungünstig, denn jetzt sind die Notfalldaten nicht verfügbar und ein Hausbesuch des Arztes oder eines Pflegedienstes wäre nicht mittels Gesundheitskarte abrechenbar.
- Die Praktikabilität dieses Ansatzes bei Hausbesuchen oder gar in Pflegeheimen scheint mir ausgesprochen fraglich. Insbesondere in Pflegeheimen und Krankenhäusern ist es schwer vorstellbar, dass Patienten ihre PIN nicht preisgeben müssen – vor dem Hintergrund der elektronischen Signatur und den damit verbundenen Möglichkeiten, wie Patientenverfügung, Testamente und Verträge rechtswirksam zu unterschreiben, sicherlich nicht ohne Brisanz[11] ...
- Wie merkt sich der Apotheker die Medikamente auf dem Weg zu den Arzneischränken? Bisher diente das Papierrezept als Checkliste und die Medikamente wurden dem Patienten an Hand des Rezepts nochmal vorgezählt – eine sehr effektive Qualitätssicherung zur Vermeidung der Ausgabe falscher Medikamente.
- Die Transparenz und Prüfbarkeit der Papierrezepte ist sehr hoch: Die große Mehrzahl der Patienten ist ohne weiteres in der Lage, die Rezepte zu lesen und mit den ausgegebenen Medikamenten hinsichtlich Zahl und Packungsgröße zu vergleichen – ein recht brauchbares Kontrollinstrument. Mit dem eRezept muß der Patient erst an ein öffentliches Terminal, um sich die Medikamente notieren, damit dann in der Apotheke die Prüfung noch möglich ist. Die Kontrollfunktion des Patienten und sein Informationsstand werden so eher geschwächt.
- Um den Risiken von Strom-, Computer- oder Datenleitungsausfällen zu begegnen, wird allerdings jedes eRezept wohl von einem Papierrezept begleitet werden müssen – so lauten zumindest die Sicherheitsanforderungen. Dies entschärft einige der obigen Punkte, wirft aber eine interessante neue Fragen auf: Wie wird die Übereinstimmung zwischen eRezept und Papierrezept sichergestellt? Wie wird die Nutzung des eRezepts dann weiter gewährleistet, denn nur dort liegt das Einsparungspotential?[12] Wie wird die Doppeleinlösung verhindert?[13]

  Dabei gäbe es ein technisch pfiffige Lösung für das eRezept: Auf das klassische Papierrezept wird ein briefmarkengroßer 2D-Barcode zusätzlich aufgedruckt, in dem die Verordnungsdaten ohne Versichertenidentifizierung nochmal codiert und vom Arzt elektronisch signiert sind – sämtliche vorgenannten Probleme verschwinden schlagartig.

4.2.2 Wechselwirkungsprüfung

Wechselwirkungs- und Verträglichkeitsprüfungen sind, richtig gemacht, aus medizinischer Sicht definitiv segensreich – allerdings genügt die Liste der eRezepte hierzu wohl nicht:

Es müssen alle relevanten Substanzen und ihre aktuelle Dosierung bekannt sein. Neben Fragen der Compliance bei der Einnahme rezeptierten Medikamente und dem völlig vorschriftsmäßigen Absetzen oder Reduzieren bei Nebenwirkungen, gibt es zahlreiche verordnungsrelevante Wirkstoffe außerhalb der Rezeptierung: Kräutertee-, Kaffee-, Milch- oder Grapefruit-Konsum sowie rezeptfreie Medikamente. Darüber hinaus gibt es verschreibungspflichtige Wirkstoffe aus schwer kontrollierbaren Quellen: die Familienapotheke, das Internet und schließlich illegale Drogen.

Ohne Befragung und Beratung des Patienten geht es also nicht – und aus Österreich ist zu vernehmen, dass dort, im Zusammenhang mit der datenschutzproblematischen Übermittlung von Vorsorgeuntersuchungsergebnissen an den Hauptverband der Sozialversicherer, die Patienten wohl beginnen, Informationen gegenüber ihren Ärzten zurück zu halten.

[10] Die Österreichischen Ärzte berichten von 30-60 Minuten, wobei dort nur die Versichertenausweisfunktion realisiert ist, so dass die Verdopplung des Zeitaufwands hoch plausibel ist, denn die Verordnung erfordert eine zweite Kartentransaktion.

[11] Selbst wenn dazu eine getrennte PIN verwendet wird: „Och, Omachen, gib' mir mal Deine PIN. Nee, das war die falsche, die andere ...“ (Übrigens: Mit 40°C Fieber oder unter starken Schmerzmitteln funktioniert das wahrscheinlich auch beim Autor!)

[12] Ein wesentlicher Nutzen liegt schließlich in der Vermeidung des Medienbruchs. Sagen sich Patienten nun „Ich habe ein Papierrezept, das löse ich ein – das andere ist mir zu unheimlich oder virtuell“ geht der Nutzen verloren.

[13] Es wird erst die Papierversion, kurz darauf die eRezept-Version eingelöst. Die Schutzbehauptung des Patienten könnte etwa sein „Ich bin glühender eCard-Anhänger, ich schmeiße diese rückständigen Papierrezepte gleich beim Arzt in die Tonnne ...“

4.2.3 Notfalldatensatz

Ein Notfallsatz erscheint spontan einfach nur sinnvoll und rundum positiv.

Ernüchternd waren dagegen die Aussagen etlicher Notärzte gegenüber dem Autor:

- Die Daten können nur Hinweischarakter haben. Trotz Blutgruppe auf dem Ausweis bleibt beispielsweise der Bluttest eben notwendig – schließlich besteht keine absolute Gewißheit über Zusammengehörigkeit von Patient und Karte.
- „Im Notfall können wir keine Zeit damit vergeuden, Patiententaschen zu durchsuchen." – „Und: wie begründen wir die Verzögerung der Notfallbehandlung, wenn wir keine oder zwei finden?"
- Bei Massenkarambolagen oder Busunfällen wird dieses Identifizierungsproblem schnell gravierend: „Wir können ja schlecht *Memory* mit Gesundheitskarten und blutverschmierten, entstellten Notfallpatienten spielen."
- „Im Notfall stehe ich mit dem Gesicht zum Patienten und nicht zum Computer." und „Wie handeln wir denn bei Computerproblemen kunstgerecht – auf die Daten eventuell zu lange warten oder ohne Daten eventuell falsch behandeln?"
- Bei größeren Katastrophen wie etwa Überschwemmungen, Erdrutschen, Lawinen, etc., wenn die Daten am dringlichsten benötigt würden, werden sie wahrscheinlich nicht verfügbar sein: entweder es fehlt der Strom oder die Technik wird durch Feldbedingungen wie Schlamm-, Sand- oder Feuchtigkeitseintrag etc. schnell versagen.

  Weiterhin sind viele chronische Krankheiten, Allergien und Wechselwirkungen erblich disponiert – mit den noch zu schildernden Risiken für Patient, Kinder und Kindeskinder. Und niemand weiß, welche Stoffwechsel-Disposition sich zukünftig aus einem bisher vordergründig harmlosen Datum wie etwa einer Acetatsalicylsäure-Unverträglichkeit ableiten läßt. Es ergibt sich somit für die Notfalldaten ein durchaus signifikanter Datenschutzbedarf.

  Wir sehen hier einen klassischen Zielkonflikt der IT-Sicherheit: Verfügbarkeit und Vertraulichkeit – sollen die sensiblen Notfalldaten streng kontrolliert oder leicht zugänglich sein?

  Sind die Daten nur mittels elektronischem Arztausweis off-line lesbar, sind sie schon außerhalb Deutschlands im Notfall nicht mehr nutzbar, denn die Gesundheitskarte ist eine nationale Lösung. Doch dieser Schutz kann leicht mittels gestohlener Arztausweise, die mangels On-Line-Prüfung nicht sperrbar sind, oder von Werksärzten, ausgehebelt werden. Verlangen wir deswegen eine On-Line-Prüfung, so sind die Daten im Notfall bei mangelnder Konnektivität unerreichbar. Setzen wir dagegen ganz auf die Verfügbarkeit und damit auf freie Zugänglichkeit, so wird jede verlorene Gesundheitskarte ein Problem und der Diebstahl attraktiv.

5 Sicherheit der Gesundheitstelematik

5.1 Schadenspotentiale und Bedrohungsannahmen

Nicht umsonst zählen Gesundheitsdaten im Europäischen und Deutschen Datenschutz zu den höchst schutzbedürftigen Datenarten. Auch andere Sicherheitsdimensionen jenseits der Vertraulichkeit verdienen im Gesundheitswesen höchste Aufmerksamkeit – ich beschränke mich hier auf einen Ausschnitt. Wir werden sehen, dass die Patientendaten in mehrfacher Hinsicht höchst schutzbedürftig sind und gleichzeitig praktisch jede Form krimineller Energie und allen denkbaren Angreifertypen ein attraktives Ziel bieten.

Zu ähnlichen Schlüssen kommen auch der Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit" der Gesellschaft für Informatik (GI) und Dr. Thilo Weichert vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein.

5.1.1 Offenlegung der Patientendaten

Eine Offenlegung von Patientendaten geht über eine massive Verletzung der Intimsphäre und der Persönlichkeitsrechte des Betroffenen weit hinaus und ist nicht nur geeignet seine „gesellschaftliche Stellung" zu gefährden sondern auch die der Kinder und Kindeskinder: Für viele Krankheitsbilder ist inzwischen eine genetische Disposition erwiesen, neue Erkenntnisse kommen laufend hinzu und es kann niemand absehen, welche a-priori harmlos wirkenden Fakten im Lichte neuer

Erkenntnisse plötzlich hochsensibel werden können. Aus der Krankengeschichten der Elternoder Großeltern lassen sich so Krankheitsdispostionen über Generationen ableiten.

Dies gefährdet die Versicherbarkeit sowohl der Patienten selbst und wie auch ihrer Nachkommen: Kranken-, Lebens- und Berufsunfähigkeitsversicherungen werden erhöhte Risiken natürlich meiden, wenn dies möglich ist. Auch Arbeitgeber werden vielleicht erhöhte Krankheitszeiten oder Frühinvaliditätsrisiken meiden wollen. Banken werden wiederum, wegen des erhöhten Ausfallrisikos und der fehlenden Lebensversicherung nur teure Kredite vergeben – auch der Weg in die Selbstständigkeit wird für die Betroffenen schwer werden.

Geschieht dies nur in Einzelfällen, so wird es als Schweigepflichtverletzung der Ärzte dieser Patienten interpretiert werden. Wir wissen aus der Geschichte der Bankautomatenkarten, wie lange Kunden, deren Karten mit PIN mißbraucht wurden, stigmatisiert wurden, ehe die (damals) völlig ungleichmäßige Verteilung der PINs, und damit ihre Ratbarkeit binnen kurzer Zeit, vor Gericht bewiesen wurde.

Geschieht es dagegen in breiter Masse, besteht die Gefahr einer Mehrklassen-Gesellschaft, in der die Menschen als „Weißglas“, „Grünglas“ und „Braunglas“ sortiert und behandelt werden.[14] Neben den schon erwähnten Erschwernissen für die Menschen mit schlechtem Morbiditätsfaktor wird es gewiß bald unappetitliche Überlegung geben, ob – zum Wohle des Landes natürlich – überhaupt noch in vollem Umfang in die Ausbildung von Grün- und Braunglas zu investieren sei, ob Brautleute nicht ein Recht auf Auskunft über den Morbiditätsfaktor der Zukünftigen haben müssten, ob – nur zum Wohle der Ungeborenen natürlich – ...

Für einen vollqualifizierten Personendatensatz inklusive der Hobbies, Konsumgewohnheiten, Einkommen und Beruf lassen sich bei interessanten Personenkreisen durchaus an die 100 € erzielen. Auch die Krankenkassen zahlen den Ärzten je DMP-Datensatz („Chroniker-Programme“) 100 €. Im Zusammenhang mit dem DMP-Skandal[15] im Januar 2005 nannten mir Ärzte Schwarzmarktpreise von mindestens 100–150 € je Datensatz, auch weitaus höhere Werte wurden genannt. Dabei stellen die DMP-Datensätze nur einen Ausschnitt der kompletten Krankengeschichte dar. Selbst die Historie der verordneten Medikamente kann einen eventuell vollständigeren Überblick über Diagnosen und Krankengeschichte eines Patienten liefern.

Schätzt man auf dieser Basis den Wert der Gesundheitsdaten aller Bundesbürger, um eine Vorstellung von der Angriffswahrscheinlichkeit und der involvierten kriminellen Energie zu bekommen, ergibt sich eine Größenordnung von 8–12 Mrd. €!

Die Vertraulichkeit der Patientendaten ist also ein hochsensibles Schutzgut, und ein hochattraktives Angriffsziel für viele – eine gefährliche Gemengelage.

5.1.2 Manipulation der Patientendaten

Werden Patientendaten manipuliert droht neben dem Verlust von Krankengeschichte bei sachkundiger Manipulation Gefahr für Leib und Leben. Dies kann, insbesondere bei Zielen mit Personenschutz, ein hochattraktives Angriffsziel für Schwerkriminelle sein, da so die Leibwächter umgangen werden können. Dazu müssen die Patientendaten garnicht zwingend selbst modifiziert werden: Es kann unter Umständen genügen, die Ausgabe auf Bildschirmen oder Druckern zu manipulieren.

Der betroffene Arzt wird sich mit der Interpretation als Kunstfehler und Haftungsfragen konfrontiert sehen, die Datenmanipulation, insbesondere bei flüchtigen Bildschirminhalten, wird er nicht nachweisen können.

Der Täterkreis dürfte eher klein sein, aber dafür um so skrupelloser in der Wahl seiner Mittel ...

[14] „Weißglas“ – Menschen mit tadelloser Gesundheitsdisposition, „Grünglas“ – mit leicht problematischer Gesundheitsdisposition, „Braunglas“ – mit stark problematischer Gesundheitsdisposition. „Milchglas“, also Menschen, deren Morbiditätsfaktor unbekannt ist, werden langfristig wie Braunglas behandelt – wären sie Weißglas, hätten sie also nichts zu verbergen, hätten sie ihre Daten ja offen gelegt, also sind sie Grün- oder Braunglas – da sie aber schlechter behandelt werden als Grünglas ...

[15] DMP-Fragebögen wurden im Auftrag der Krankenkassen von einem Privatunternehmen gescant und augenscheinlich unverschlüsselt über das Internet nach Vietnam zur Erfassung (also Abtippen) versandt. Dort sollen sie nach der Erfassung „zweitverwertet“ – also an internationale Pharmakonzerne verkauft worden sein. Es ermittelt(e) die Staatsanwaltschaft. Laut Auskunft einiger Ärzte soll dieser nach Sozialgesetzbuch eigentlich gesetzeswidrige Vorgang durch eine Änderung des SGB im Eilverfahren nachträglich legitimiert worden sein ...

5.1.3 Unbefugter Zugriff auf Praxis- oder Klinik-IT

Kernmoment der Gesundheitstelematik ist die Vernetzung aller Praxis- oder Klinik-IT untereinander sowie der Datenaustausch untereinander. Selbst wenn diese Vernetzung als geschlossenes Netz implementiert würde, unterscheidet es sich hinsichtlich der vielen Teilnehmer, Zugangswege, Protokolle und Austauschformaten nur quantitativ aber kaum qualitativ vom Internet.

Damit sind alle bekannten kommunikationsbasierten Angriffsstrategien gegen die eingebundenen Praxis- und Klinik-IT-Systeme möglich und können – je nach lokaler IT-Sicherheit[16] – die Risiken der Offenlegung und Manipulation von Patientendaten auch dort und auch für Daten auslösen, für die keine Einwilligung zur Verwendung innerhalb der Gesundheitstelematik erteilt wurde.

Darüber hinaus wird die Sabotage und Lähmung des Praxis- oder Klinikbetriebs möglich – ein hochattraktives Angriffsziel für terroristische Gruppen, kann doch über diese Hebelwirkung der Blutzoll eines Anschlags oder auch natürlicher Katastrophen oder Epidemien dramatisch verstärkt werden.

Allerdings lehren die Erfahrungen in Österreich, dass auch schon die ganz normalen Abhängigkeiten und Pannen vernetzter Systeme erhebliche Betriebsstörungen bedingen können ...

5.2 Einige Erfahrungswerte

Da es die Gesundheitstelematik als solches eigentlich noch garnicht gibt, sollen Erfahrungswerte mit hochsensiblen Daten andernorts, mit kritischen Infrastrukturen und Systemen in Deutschland und mit der Gesundheitstelematik eng verwandten Projekten einen Eindruck vermitteln, mit welchen Schwierigkeiten und Risiken ergänzend zu der eher theoretischen Schadpotentialbetrachtung in der Praxis zu rechnen ist.

5.2.1 Internationaler Stand der IT-(Un)-Sicherheit

Eine vollständige Liste aller spektakulären IT-Sicherheitspannen weltweit wäre sicherlich ein interessantes Lesefutter für sich und könnte lässig ein Buch füllen – das sei hier garnicht erst versucht. Ich beschränke mich hier auf jüngere, besonders interessante Ereignisse, bei denen klar wird – und das ist wirklich ohne jede Häme gegenüber den Betroffenen gemeint! –, dass selbst gut ausgestattete Profis bei klar erkannten, mit erheblichem Einsatz bewußt verfolgten Schutzzielen mit dramatischem Schadenspotential dennoch versagen können:

- Monatelang plündert „Titan Rain“ sensible Daten aus Systemen der US-Behörden und des -Militärs sowie von Systemen der Briten, und zwar trotz Gegenwehr!
- Sony BMG verteilt sein brandgefährliches „Root-Kit“ über Wochen, ohne das Sicherheitsdienstleister wie die Antivirenhersteller vertragsgemäß ihre Kunden warnen – was per se schon durchaus spannende Fragen aufwirft ...
- Zig Millionen Kreditkartendaten werden direkt an der Quelle gezapft ...
- Das BSI verteilt „Sober.L“ via seiner CERT-Mailing-Liste.
- 2001 wurde die SmartCard-basierte elektronische Signatur-Lösung der Signtrust (BSI-zertifizierte SW „eTrust“) durch Bonner Informatiker geknackt.[17]
- ...

5.2.2 e-Card Austria

Es liegt nahe zu unserem Nachbarn Österreich und dessen e-Card-Projekt zu schauen. Immerhin sind im wesentlichen die gleiche Technologie im Einsatz und die gleichen deutschen Unternehmen mit der Umsetzung betraut. Allerdings ist der Funktionsumfang deutlich geringer als in der deutschen Gesundheitstelematik geplant, denn es wird nur der Versichertenausweis und die Leistungsabrechnung über die e-Card Austria abgewickelt.

[16] Die laut Bundesdatenschutzbeauftragten Herr Schaar ja besorgniserregend ist ...

[17] Dieses kleine Lehrstück verdient etwas Erläuterung, da es für die Gesundheitstelematik gleich in mehrererlei Hinsicht hochrelevant ist: Durch Angriffe auf der Betriebssystemebene konnte den Benutzern zum einen ein beliebig anderes Dokument angezeigt werden, als von der Chipkarte signiert wurde. Weiterhin konnte die PIN abgefangen und, solange die Chipkarte im Zugriff war, zur programmatischen Signierung beliebiger Dokumente mißbraucht werden. Die frühzeitigen Warnungen der Informatiker Monate vorher an BSI, RegTP und Deutsche Post (Mutter von SignTrust) waren augenscheinlich ignoriert worden, so dass sich die Informatiker gezwungen sahen, die öffentliche Ankündigung, hier sei nun ein sicheres Signiersystem verfügbar, zu kommentieren. Ebenfalls aufschlußreich war der Umgang mit den Kritikern sowie die wirtschaftliche Entwicklung von SignTrust ...

Trotz des geringeren Ehrgeizes im Funktionsumfang gibt es einen möglichen Vorgeschmack:

- Sozialhilfeempfänger erhielten keine e-card, so dass ihr Sozialhilfestatus klar erkennbar war.
- Abrechnungs- und Verordnungsdaten des Arztes lassen Rückschlüsse auf die Krankengeschichte des Patienten zu.
- Die Datenbanken des Hauptverbandes der Sozialversicherer, die nun Morbiditäts- und Risikofaktoren enthalten, können durch Versicherungen und Arbeitgeber zugegriffen werden – natürlich nur mit „freiwilliger Zustimmung" der Bürger ...
- Das Vertrauensfundament in die Ordnungsmäßigkeit des Projekts hat Risse: Kritik des Österreichischen Rechnungshofes, „Gehaltsskandale" und „Undurchsichtigkeiten" bei zentralen Protagonisten, Vorwürfe über geheime Absprachen bei der Ausschreibung, etc.
- Es gibt ernste Probleme mit der Stabilität und Zuverlässigkeit, so etwa die Totalausfälle am 24.+26.09., 14.12.05, ... und kontinuierlich zahlreiche regionale oder lokale Störungen
- Außerordentlich empfehlenswert: das e-card-Tagebuch bei www.hausaerzteverband.at! Neben der für sich schon hochspannenden Wandlung vom Enthusiasmus eines freiwilligen Teilnehmers des österreichischen Modellversuchs im Jänner 2005 zur Ablehnung heute, gibt es tiefe Einblicke in Verläßlichkeit und Störbehebungsaufwand und dessen Einfluß auf die Praxis: „Ich muß mich mehrmals täglich daran erinnern, dass meine Aufmerksamkeit den Patienten und nicht den Computern gelten muß". Skurile Anekdoten über das Zusammentreffen der Daten und der realen Welt, wie etwa die langjährige Patientin, die plötzlich – leibhaftig vor dem Arzt stehend – als tot vermeldet wird u. v. a. m.
- Die Österreichischen Ärzte drohen angesichts ihres enormen Zusatzaufwands und der Unzuverlässigkeit inzwischen offen mit dem Ausstieg aus dem System.

5.2.3 Kritische Infrastrukturen und Systeme in der Bundesrepublik

Von der Illusion, es gäbe in Deutschland beispielsweise keine flächendeckenden Stromausfälle haben wir uns nach den regionalen Stromausfällen in 2004 und 2005 ja wohl verabschiedet.[18]

Ausfallende Internet-Konnektivität und aus vielfältigen Ursachen kollabierende IT-Infrastrukturen hat jeder von uns sicherlich häufiger und ernster erlebt als wünschenswert – selbst wenn wir davon leben.

Leuchttürme der Public-Private-Partnerships, Meisterstücke deutscher Technologiekonzerne, Innovationsinitiativen und Exportschlager haben wir in Form von ALG II Software, Toll-Collect, InPol Neu, Herkules, FISCUS, ELSTER, ... ausreichend. Wir brauchen unseren internationalen Ruf also nicht mit der Gesundheitstelematik weiter zu festigen oder gar auszubauen.

Die Beständigkeit gesetzlich verordneter Nutzungs- oder Verarbeitungsverbote konnten wir am Beispiel des DMP-Skandals oder der Diskussion über die Aufhebung der Zweckbindung der Maut-Daten verfolgen.

Der Verkauf der Kontaktdaten von Temo-Sündern, die daraufhin mit Radar-Warner-Werbung überflutet wurden, zeigte, dass auch Behördenmitarbeiter für Nebenverdienste gewinnbar sind.

All dies sind Beispiele aus der Bundesrepublik – mit anderen Staatsgebilden auf deutschem Boden will ich garnicht ins Detail gehen. „So etwas kann bei uns in Deutschland nicht passieren" ist eine Formulierung, die besser außer Gebrauch genommen würde ...

5.2.4 Konkrete Analyse eines Vorprojekts der Gesundheitstelematik

Es gibt – auch wenn der **Hersteller des Systems meine Ergebnisse bestreitet** – durchaus Anlaß an der Sicherheit mancher Vorprojekte zur Gesundheitstelematik zu zweifeln:

2003 geriet ich zufällig an einen Untersuchungsauftrag, in dem es ein System zum Austausch medizinischer Daten zwischen Arztpraxen und Kliniken – also durchaus etwas was als Vorprojekt der Gesundheitstelematik bezeichnet werden kann – auf Sicherheitsmängel hin zu untersuchen

[18] August 2004: weite Teile von Rheinland-Pfalz, Saarland, Luxembourg und Nord-Belgien 4–8 Stunden ohne Strom – ein Kaskadenversagen: nach dem Abschalten einer von drei Hauptleitungen, brach eine zweite zusammen, woraufhin auch die letzte wegen Überlast notabschaltete (n+1-Redundanz ist halt zu wenig ;-). Laut RWE war die genaue Ursache nicht feststellbar ... (Außerdem erkannte die Landesregierung RLP: Mobiltelefone sind kein taugliches Krisenmanagementinstrument ;-)
November 2005: Teile des Münsterlands, teils mehr als 4 Tage ohne Strom – Kollabieren von Leitungen unter Schneelast. Laut RWE: „höhere Gewalt" (naja, und ein paar ignorierte Materialprobleme ;-)
Die RWE hat aber auch Pech ...

galt. Der Auftraggeber A wollte dies als unabhängigen Teil der Qualitätssicherung der gelieferten SW eines Herstellers B – beide werde ich nicht benennen.[19]

Der Untersuchungsauftrag war mit 4 Tagen für eine reine Black-Box-Analyse äußerst knapp bemessen und ich wies ausdrücklich auf die dadurch mögliche geringe Untersuchungstiefe und die Unwahrscheinlichkeit verwertbarer Ergebnisse hin – insbesondere da das System intensiven Gebrauch von Kryptographie machte, sogar Smart-Cards einsetzte, das Placet der Datenschützer hatte, aus durchaus namhaften Hause kam und augenscheinlich schon länger praktisch eingesetzt wurde, rechnete ich mir nicht die geringste Chance aus, irgendeine Schwachstelle zu finden.

Ich hatte mich getäuscht ...

Um den zeitlichen Systemablauf besser zu verstehen, zeichnete ich die Kommunikation mit dem Chipkartenleser auf. Zu meinem größten Erstaunen erfolgte diese nur bei Start der System. Spätere Signier- und Entschlüsselungsvorgänge griffen nicht auf die SmartCard zu – diese ließ sich sogar entnehmen, ohne das dies irgendeine Änderung im Systemverhalten verursachte. Dies ließ nur den Schluß zu, dass hier die eigentlich produktiven Private-Keys etwa der Ärzte nicht im sicheren Kryptomodul der SmartCard lagen, sondern diese als Speicherkarte mißbraucht und die Private-Keys ins System hochgeladen wurden – also auf der seriellen Leitung per SW abgreifbar sind.

Damit wären dann allerdings elektronische Arztunterschriften fälschbar, somit Patientendaten und Vorgänge manipulierbar – und in Konsequenz die Rechtsverbindlichkeit und Nachvollziehbarkeit der Behandlungsvorgänge im Modellversuch in Frage gestellt.

Die Patientendaten selbst waren aber nochmals durch ein „Ticket“ geschützt, eine Zeichenkette, aufgedruckt auf dem Überweisungsschein. Nur mit diesem Ticket ließen sich die Daten von einem zentralen Server herunterladen und lokal entschlüsseln – eine der Kernsicherheitszusicherungen war, dass der Server-Betreiber eben wegen dieser Verschlüsselung außer Stande sei, in die Patientendaten Einsicht zu nehmen, ja, sogar für jeden Zugriff auf die Daten die Einwilligung des Patienten unabdingbar sei.

Ein erster Blick auf diese „Tickets“ sorgte für Stirnrunzeln – die effektive Schlüsselbreite lag bei etwa 109 Bit – eigentlich schon etwas dürftig. Doch dann die Überraschung: Ein Großteil des Tickets war eine klar strukturierte, vorhersagbare Vorgangskennung – übrig blieben nurmehr etwa 25 Bit unaufgeklärte Schlüsselbreite: eindeutig zu wenig und brute-force-zugänglich. Nachdem ich einige hundertausende Tickets mit Zeitstempeln hatte erzeugen lassen, zeigte sich in der Korrelationsanalyse eine ganz klare Zeitabhängigkeit mit Sekundenauflösung. Es ließ sich, anhand der Korrelationsmuster, durch Probieren recht schnell ein Programm finden, welches jeweils die Tickets an Hand des zeitstempels rekonstruieren konnte – jetzt bräuchte ein Angreifer eigentlich nurmehr die Zeit der Ticket-Generierung zu raten, eigentlich kein Problem per Brute-Force.

Allerdings gab es einen viel einfacheren Weg: Um die Dateinamen zu verschleiern, wurden alle Dateien in einen Zeitstempel umgenannt. Die jeweils älteste Datei in einem Vorgang markierte den Zeitpunkt des Verbindungsaufbaus beim Anlegen des Vorgangs – also den Zeitpunkt der Ticket-Generierung – mit höchstens wenigen Sekunden Abweichung ...

Dieser Zeitpunkt war dem Systembetreiber oder jedem mit Zugang zu einem Arzt-Client im Dateinamen zugänglich. Damit kann aber das Ticket berechnet und in die Client-SW eingegeben werden, also augenscheinlich ohne Patientenmitwirkung Patientendaten eingesehen werden ...

Darüber hinaus konnte ich in den offiziellen Dokumenten weder irgendwelche Härtungsanweisungen für die Systeme finden, noch eine Forderung nach Firewalls – im Gegenteil wurden diese als unnötig bezeichnet, da ja nur über ISDN kommuniziert werde. Damit ist angesichts der unbeschränkten TCP/IP-Kommunikation und ungehärteter früher MS-Windows-Versionen der Erfolg von Remote-Angriffen über diese Verbindungen extrem wahrscheinlich – ein einziger kompromittierter Rechner im gesamten geschlossenen Netz würde alle anderen ernsthaft gefährden.

Wie gesagt: **Der Hersteller des Systems bestreitet die Richtigkeit meiner Ergebnisse.**

[19] A und B streiten vor Gericht. A hat mein Gutachten als Parteigutachten eingebracht – ohne meine Zustimmung oder Zutun, diese Verwendung liegt schlicht im Ermessenspielraum eines Auftraggebers solcher Studien. Da das Gutachten damit quasi öffentlich war, bat ich A Monate später, es für einen didaktischen Vortrag über Nutzen und Vorgehensweise von Sicherheitsanalysen beim CCC als Beispiel verwenden zu dürfen – was mir unter der Auflage keine Namen oder Produkte zu nennen gewährt wurde. Der eigentliche Vortragszweck ist in der öffentlichen Rezeption des Vortrags allerdings etwas untergegangen ...

5.3 Verbesserte IT-Sicherheit!?

Der Bundesdatenschutzbeauftragte Herr Schaar sieht reichlich IT-Sicherheits- und Datenschutzprobleme in bestehenden Praxis- und Klinikcomputersystemen und erhofft sich, dass die Einführung der Gesundheitstelematik eine große Verbesserung bewirkt. Diese Hoffnung bedarf allerdings zumindest ausführlicher Begründung – denn Vernetzung, impliziert mit der Gesundheitstelematik, steht ja nicht gerade im Ruf, der IT-Sicherheit unmittelbar förderlich zu sein.

Tatsächlich meiden daher sehr viele Ärzte[20] aus gesundem Mißtrauen jede Vernetzung nach Außen. Viele lassen keine Fernwartung zu, obwohl sie für diese Sicherheitsmaßnahme zugunsten ihrer Patientendaten höhere Wartungskosten tragen müssen. Wenn Internet-PCs benötigt werden, so sind sie in aller Regel komplett vom Praxisnetz getrennt[21], und über Ärzte, die in Foren anderes berichten, bricht eine Flut kollegialer Warnungen herein.

Zugegebenermaßen kommen mir teilweise auch wirklich erschreckende und gefährliche Konstruktionen, wie etwa unverschlüsselte Praxis-WLANs, zu Ohren. Doch war hier bisher immer ein (überbordender) Vertrauensvorschuß in die Sachkunde und das Sicherheitsbewußtsein von „IT-Experten“ am Werk und nach Erläuterung der Risiken eine kompromißlose Bereitschaft zur Absicherung klar erkennbar – wäre eine solche Priorisierung der Sicherheit verbreiteter, wir hätten signifikant weniger Probleme ...

Vor diesem Hintergrund der großteils sehr vernünftigen IT-Sicherheitsgrundhaltung der Ärzte verdienen sie meines Erachtens eine sehr detaillierte Erklärung, wieso durch die Einführung der Gesundheitstelematik die Sicherheit ihrer Systeme steigen soll und zwar auf ein bisher international unerreichtes Niveau – insbesondere, weil die Rahmenarchitektur, wie wir noch sehen werden, nur Grundschutz für diese Systeme ansetzt und selbst besser gesicherte Systeme erfahrungsgemäß entschlossenen Angreifern, wie etwa „Titan Rain“, nicht standgehalten haben.

Und wir alle verdienen rückhaltlose öffentliche und offene Tests der effektiven Sicherheit als Vorbedingung für den Einsatz mit echten Patientendaten – auch schon für die Modellversuche!

5.4 Sicherheitsanforderungen der bit4health-Rahmenarchitektur

Als ich die Sicherheitsanforderungen der bit4health-Rahmenarchitektur las, tat ich das eigentlich in der Absicht, mir selbst zu beweisen, dass das von mir untersuchte System ein katastrophaler Ausreißer war, mit der Sicherheit der Gesundheitstelematik überhaupt nicht zu vergleichen sei und mich so zu beruhigen ...

Ich stütze mich auf die Dokumente der Rahmenarchitektur bei www.dimdi.de in der Version 1.1. Diese Rahmenarchitektur wurde wiederholt als verbindliche Grundlage der noch zu entwickelnden Lösungsarchitektur bezeichnet. Die Sicherheitsanforderungen sind mit 62 Seiten nur ein überschaubar kleiner Teil der über 1000 Seiten – ich empfehle jedem eindringlich, sie selbst zu lesen und sich ein eigenes Urteil zu bilden.

Es sei voraus geschickt, dass die Autoren das Sicherheitshandwerk durchaus verstehen – die Probleme liegen wahrscheinlich eher in den Vorgaben.

5.4.1 Richtig gute Sicherheitsanforderungen

Es gibt eine ganze Reihe wirklich vorbildlicher Anforderungen – wir werden nur leider später ihre Verletzung feststellen müssen:

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) Für jeden neuen und veränderten Geschäftsvorfall soll ein analoger, papierbasierter Prozess existieren. ...

[20] Stichprobe: etliche Dutzend, die ich inzwischen auf zahlreichen Vorträgen und Diskussionen kennengelernt habe, sowie weit mehr in einschlägigen Foren ...

[21] Layer-1-Firewall: keine physische Verbindung

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.**

5.4.2 Widersprüchliche Einstufung des Schutzbedarfs

Nach den geschilderten Schadpotentialen ist offenkundig, dass die Gesundheitstelematik im BSI-GSHB-Schutzbedarf-Schema praktisch durchgängig als hoch bis sehr hoch einzustufen ist. Diese Einschätzung wird in den Sicherheitsanforderungen (p. 25, oben) auch vertreten:

> **Zusammenfassend kann daher der Schutzbedarf der durch die Telematikprozesse unterstützen Prozessschritte als *hoch* bis *sehr hoch* eingestuft werden,**

Hier zum Vergleich die GSHB-Schutzstufen:

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.

Dem steht dann allerdings folgende Einstufung aus den Sicherheitsanforderungen entgegen:

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.

…

Die bestehenden Praxis- und Kliniksysteme, sind natürlich Kernkomponenten aller Geschäftsprozesse und als Orte der Wahrnehmung, Pflege und Zugriffskontrolle für Patientendaten auch entscheidend für deren Sicherheit. Diesen Systemen wird nur ein niedriger bis mittlerer Schutzbedarf zu gesprochen – obwohl eindeutig Datenmißbrauch mindestens erhebliche Auswirkungen haben kann und eine Gefahr für die persönliche Unversehrheit ohne weiteres denkbar ist. Insbesondere wird unterstellt, dass die bisherigen Maßnahmen und Sicherheitskonzepte ausreichend seien –

dass aber ist hochgradig fraglich, denn die Gesundheitstelematik erzwingt eine umfassende Vernetzung und neutralisiert dadurch gerade alle Maßnahmen, die auf Konnektivitätsverzicht basieren – also die Kernkomponente vieler Sicherheitskonzepte zumindest in Arztpraxen.

5.4.3 Informationshoheit der Patienten?

Die folgende Forderung stellt sowohl die vollständige Informationshoheit der Patienten (PAS-17) wie auch das Prinzip, die Sicherheit nicht auf einzelne Personen zu gründen (RAS-4) in Frage:

> **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)

Es gibt also augenscheinlich Nachschlüssel, die den Datenzugriff sehr wohl ohne Mitwirkung des Patienten gestatten – und dieser hochbrisante Schlüssel ist einer Person anvertraut. Angesichts der mit diesem Schlüssel geschützten Werte möchte ich mit dieser Person nicht tauschen: Sparkassendirektoren haben aus gutem Grund keine alleinschließenden Tresorschlüssel mehr, weil Ihre Familien schon für weitaus geringere Werte als Geiseln genommen wurden.

Auch diese Forderung deutet Zugriff ohne Patientenbeteiligung an – und damit im Zweifelsfall auch gegen den Willen des Patienten:

> **ZAS-5** **Unautorisierte Übertragung von Daten(-segmenten) der eGK:** In Ausnahmefällen muss eine Übermittlung von Patientendaten an die GKV sichergestellt werden (Schadensersatzansprüchen gegenüber Dritten). ...

Noch ernster und von größerer Tragweite scheint aber folgendes Zitat:

> **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). ...

Es ist also geplant, die Krankengeschichte eines Patientenpseudonyms über die Zeit zu verfolgen und daran detaillierte Auswertungen vornehmen zu können. Natürlich gibt es sinnvolle Anwendungen wie Statistiken oder medizinische Forschung – allerdings impliziert es, dass die Daten zentral entweder unverschlüsselt oder per universellem Nachschlüssel entschlüsselbar gespeichert werden (wobei letzteres aus Performance-Gründen eher unwahrscheinlich ist).

Wer solche Auswertungen durchführen darf, ist im SGB etwas unscharf formuliert – zumindest die Krankenkassen sind klare Kandidaten.

Der einzige Schutz der Patienten ist dabei ein Pseudonym, welches im Wesentlichen aus Geburtsdatum, Geschlecht und Postleitzahl besteht – und damit erheblich die Gesetzesvorlage überschreitet, in der nur Geburtsjahr, Geschlecht und Postleitregion als Pseudonym genannt wird.

Natürlich verdient ein solches Pseudonym den Namen nicht, denn es ist praktisch ein Primärschlüssel für Personendatenbanken. Statt theoretischer Herleitung sei dies an einem historischen Beispiel illustriert: Die Zentrale Personendatenbank der DDR[22] nutzte als Primärschlüssel die Personenkennziffer, die aus Geburtsdatum, Geschlecht und Melderegisterstelle bestand – wobei die heutigen Postleitbereiche eher kleiner sind als die Einzugsgebiete der Melderegisterstellen.

Dieses „Pseudonym“ birgt erhebliche Gefahren, da es direkte Abfragen zu einer Person ermöglicht: Jedem Arbeitgeber, jedem Versicherungssachbearbeiter liegen Geburtsdatum, Geschlecht, Geburtsort und Wohnort vor – damit ist direkt die Konstruktion der möglichen „Pseudonyme“ möglich, und damit wiederum die „individuelle Auswertung“.

Hauptproblem sind nun nicht mehr Angreifer von Außen, sondern Innentäter, die ihre Systembefugnisse mißbrauchen, Inferenzattacken fahren und diese Dienstleistung eventuell verkaufen ...

[22] die pikanterweise am 1.1.1984 offiziell in Betrieb genommen wurde – wie konnte George Orwell das wissen!?!

5.4.4 Mangelnde Beherrschbarkeit des Systems und des Schadenspotentials

Eine Selbsteinschätzung der Sicherheitsarchitekten zur Beherrschbarkeit des Systems im Schadensfalle liest sich so:

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.

...

Ich kann dies nicht anders interpretieren, als dass beispielsweise im Falle eines erfolgreichen Angriffs, die Ausbreitung der Angreifer und der gestiftete Schaden nicht mehr kontrollierbar sind – bei dem vorhandenen Schadenspotential würde ich einem Kunden daher äußerst dringend abraten, dieses System in dieser Form zu betreiben.

6 Bedenkenswertes und Bedenkliches

6.1 eMobbing *oder* „Sag mir Dein Scoring und ...“

Was Versicherungen mit solchen Daten anfangen können, läßt folgendes Zitat von Ellis Huber, vormals Vorsitzender der Ärztekammer Berlin, jetzt Vorsitzender der Securvita BKK, erahnen:

"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. (http://www.aerztlichepraxis.de/artikel?number=1110901029)

6.2 Der 21C3-Vortrag und seine Folgen

Wie erwähnt, verblaßte das eigentliche Kernthema meines Vortrags auf dem 21. CCC im Dezember 2004 – wie funktioniert eine Sicherheitsanalyse und wem nutzt sie? – in der öffentlichen Wahrnehmung völlig neben dem gewählten Beispiel.

Neben einer statistisch schwer bewertbaren Verdichtung unangenehmer Zufälle in meinem Leben, gibt es eine Reihe interessanter, belegbarer Fakten:

So hatte schon am 10. Januar ein Journalist Hypothesen zu Auftraggeber, System, Systemhersteller, Motivationen und einem ominösen Verbot[23] – angeblich auf Basis von Insider-Informationen, ohne jedoch mit mir oder meinem Auftraggeber, den einzigen Insidern des Auftrags, gesprochen zu haben. Dieser Journalist kam zu dem Schluß mein Gutachten sei zu ignorieren.

Als Eitel Dignatz ein halbes Jahr später im Linuxmagazin in einem Gastkommentar zu öffentlichen IT-Projekten jedoch diese Angaben als ein Beispiel zitierte und dabei zur gegenteiligen Einschätzung kam, wurde er von der Rechtsabteilung der Fraunhofer Gesellschaft zur Unterlassung aufgefordert, sogar mit nachweislich falschen Angaben über mich – vergeblich übrigens.

Auch mir blieb solche Post natürlich nicht erspart, aber der Ablauf verdient durchaus detailliertere Schilderung: Ich erhielt die Einladung, meinen Vortrag am 9.4.2005 in der Charite vor Ärzten zu wiederholen[24]. Am 8.4., gegen 15 Uhr – ein Zeitpunkt also, zudem ich, wollte ich morgens in Berlin sein, natürlich schon außer Haus sein mußte – ging bei mir per Fax eine anwaltliche Unterlassungsaufforderung ein, in der die Fraunhofergesellschaft als Auftraggeber benannt und mir unwahre Aussagen zum PaDok-System der FhG unterstellt und untersagt wurden – mit Androhung sofortiger Schadensersatzforderungen, sollte ich den Vortrag nochmals halten. Außerdem kam zu dem Vortrag in Berlin Herr Bresser, Projektleiter des PaDok-Projekts am FHG IBMT in St. Ingbert, um – wie gegenüber dem Veranstalter ausdrücklich betont, als offizieller Vertreter, den Ruf des Instituts und des PaDok-Systems zu schützen. Die FhG nutzte seine Anwesenheit

[23] Angeblich sei es mir durch den Auftraggeber verboten gewesen, den Hersteller zu kontaktiern. Dies ist unwahr – es wäre im Gegenteil, außer bei sehr guter Begründung und juristischer Absicherung, Ablehnungsgrund für den Auftrag gewesen.

[24] Was durchaus größere Umbauten des Vortrags bedingte ... mich aber auf den beeindruckenden historischen Boden des Sauerbruch-Hörsaals brachte – ein steiler Trichter, wie man ihn aus alten Schwarz-Weiß-Filmen kennt ... – ein echtes Erlebnis!

aber nicht, um eine eigenhändige Zustellung der Unterlassungsaufforderung zu versuchen oder sich über deren Kenntnis bei mir zu informieren.

Augenscheinlich gab es aber seitens Herr Bresser nichts zu beanstanden, weder während des Vortrags noch in der anschließenden Diskussion noch in der Podiumsdiskussion.

Nachdem mein Anwalt seinen Standpunkt und unsere Bereitschaft, außer wie vor Gericht zur Klärung bereit zu stehen, kollegial dargelegt hatte, setzte die FhG auch ihre juristischen Drohungen nicht um.

Der MEDI-Verbund, eine Ärztevereinigung, nahm sich aber der Sache an, indem er – vor dem Hintergrund des Heilbronner Modellversuchs – der FhG anbot, folgende Untersuchung zu finanzieren: Ich sollte in einer White-Box-Analyse PaDok auf Übereinstimmung mit meinem Gutachten überprüfen – wobei ich eventuell Irrtümer dann natürlich öffentlich richtig gestellt hätte. Sollten sich dagegen Sicherheitsmängel bestätigen, wäre von MEDI zusätzlich die Überprüfung der aktuellen SW-Version auf die Beseitigung dieser Mängel finanziert worden. Ein meines Erachtens sehr großzügiges und konstruktives Angebot, welches leider seit über einem halben Jahr ungenutzt im Raum steht.

6.3 Bürgerrecht und Bürgerpflicht

Eine technologieabhängigen Gesellschaft kann meiner Meinung nach nur dann demokratisch bleiben, wenn der Bevölerung eine freie Meinungsbildung auch in Sachfragen möglich bleibt. Diese Fragen können zunehmend nur noch von wenigen Experten mit erheblichen Zeitaufwand bearbeitet werden. Ein Großteil dieser Experten wird dabei immer in der Industrie, damit in den Eigeninteressen des Arbeitgebers, beruflich und inhaltlich gebunden sein. Um so wichtiger scheint mir daher der Schutz unabhängiger Experten vor Repressionen, wenn sie Kritik äußern: Die Mittel und die Zeit, die sie einsetzen können, halten ohnehin keinem Vergleich mit Konsortien stand – die Waagschalen neigen sich stark auf Seiten der Konzerne. Als Gesellschaft müssen wir Repressionen und Ad-Hominem-Attacken gegen solche Warner mindestens massiv ächten, eventuell durch Ausschluß aus öffentlichen Ausschreibungen analog der Anti-Korruptionslisten.

Wer sich sachlicher Kritik der Bürger nicht stellt, dem sollten wir meiner Meinung nach unser Gemeinwohl und erst recht unsere Gesundheitsdaten nicht anvertrauen!

7 Zur Person

Thomas Maus kam vor mehr als einem Vierteljahrhundert im Rahmen eines Schulversuches mit der IT in Kontakt – zu Zeiten also, als IT noch EDV hieß, man seinen ersten Computer noch selbst lötete, auf Lochkarten programmierte und Programme sehr sorgfältig plante, weil jeder Fehler im nächtlichen Batch-Lauf einen Tag Verzögerung brachte und die Ressourcen zu kostbar waren, um Machbarkeit durch Scheitern zu prüfen. Im Schülerteam, welches die Programmierung und Pflege eines Schulverwaltungsprogramm für RLP betrieb, erlebte er sehr früh hautnah professionellen IT-Einsatz und IT-Sicherheitsfragen – eine anhaltende Leidenschaft begann.

Er ist Diplom-Informatiker und studierte an der Universität Karlsruhe, wobei er den Schwerpunkt auf IT-Sicherheit am Europäischen Institut für Systemsicherheit intensiv nutzte.

Seit über einem Dutzend Jahren berät er freiberuflich Unternehmen aller Größenordnungen hauptsächlich in IT-Sicherheitsfragen und kann inzwischen auf einen bunten Strauß spannender und anspruchsvoller Aufgaben zurückblicken.