IT-Sicherheit in der Medizin

Prof. Dr. Klaus Pommerening
Institut für Medizinische Statistik und Dokumentation
Johannes-Gutenberg-Universität Mainz

Im Gegensatz zu anderen Bereichen stehen die Bemühungen um die Sicherheit der Informations- und Kommunikationstechnik in der Medizin noch am Anfang. Es gibt mehr Probleme als erfolgreiche Lösungen. Sicherheitsbedenken werden von der Welle der Computer-Euphorie überrollt. Vielen Lippenbekenntnissen, vor allem zum Datenschutz, steht eine völlig unzureichende Praxis gegenüber. Insbesondere gibt die Datenhaltung und -verarbeitung auf PCs zu ernsten Sorgen Anlaß. Dabei sind für viele der Probleme theoretische, oft sogar praktische, Lösungen vorhanden und warten nur auf die Umsetzung oder den Einsatz. Auf der anderen Seite gibt es aber auch Sicherheitsprobleme, die nur schwer zu lösen sind, oder wo die Theorie sogar die prinzipielle Unlösbarkeit beweist.

In diesem Vortrag werden die wichtigsten Sicherheitsprobleme behandelt, mit denen sich die Medizin-Informatik auseinandersetzen muß, und einige Konzepte zu ihrer Lösung vorgestellt.

1 Sicherheitsprobleme der Medizin-Informatik

Die Sicherheitstechnik für die informationsverarbeitenden Systeme in der Medizin muß sich mit zwei grundsätzlichen Problemkreisen auseinandersetzen:

- Sicherheit für den Patienten,
- Datenschutz.

Hier einige Beipiele für den ersten Problemkreis; viele weitere findet man in den Archiven der Netnews-Gruppe ‘comp.risks’ [10]:

- Durch Fehler in dem Bestrahlungsgerät Therac-25 kamen zwischen 1985 und 1987 mindestens 2 Menschen ums Leben und mehrere wurden geschädigt. Die Software konnte sich bei sehr schneller Tastatur-Bedienung bei einer bestimmten Tastenfolge „verheddern“ und die resultierende hohe Überdosis wurde nicht abgefangen.

- Ein Überwachungssystem für Intensiv-Patienten wurde vom Hersteller zurückgezogen, weil die Software die Daten nicht immer den richtigen Patienten zuordnete [1].

- Anfang 1992 wurde North Staffordshire Hospital Centre festgestellt, daß aufgrund eines Programmierer-Fehlers 10 Jahre lang insgesamt 989 Krebspatienten von einem Radiotherapiegerät mit einer 10 – 30% zu geringen Dosis bestrahlt wurden [10, Vol. 13.12].

- In letzter Zeit häufen sich Meldungen über Fehlfunktionen elektronischer Geräte durch elektronisches Störfeuer, das etwa von Mobiltelefonen oder dem allgemeinen Elektrosmog ausgeht. So versagte z. B. ein Herzschrittmacher durch die elektronische Diebstahlsicherung eines Kaufhauses [1][7].

Als Beispiele für den zweiten Problemkreis, den Datenschutz, seien einige Punkte aus einer Beanstandungsliste zitiert, die der Landesdatenschutzbeauftragte nach der Begehung einer Klinik aufstellte:

- Eingangstür ohne Sicherheitsschloß.

- Akten in hölzernen Rolltürschränken.

- Akten stapelweise auch über Nacht am Arbeitsplatz.

- Arbeits- und Backup-Disketten nicht getrennt in Trog am Arbeitstisch.

- PC-Zentraleinheit frei beweglich.

- Festplatte fest eingebaut.

- PC ohne Datenschutzsoftware.

- Keine schriftlichen Verpflichtungen auf Datenschutz.

- Keine schriftlichen Dienstanweisungen für die Mitarbeiter.

Viele weitere grundsätzliche und konkrete Probleme werden in den folgenden Abschnitten genannt.

1.1 Die Sicherheit elektronischer Dokumente

Die elektronische Patientenakte

Der erste und wichtigste Nutzen eines Computers in einer Arztpraxis oder einem Krankenhaus ist die Verwaltung der Patientendaten. Diese entstehen aus der ärztlichen Dokumentationspflicht und unterliegen der ärztlichen Schweigepflicht und den Datenschutz-Vorschriften. Ferner müssen sie (in der Regel für 10 Jahre) archiviert werden. Als Folge davon sind sie nach dem Stand der Technik bestmöglich zu schützen, wobei aber auch das Prinzip der Verhältnismäßigkeit zu beachten ist. Militärische Sicherheit ist im Krankenhaus nicht angebracht. Es muß aber gewährleistet sein, daß nur der Arzt und sein Behandlungsteam die Patientenakte lesen können. Konkrete Gefahren und mögliche Schutzmaßnahmen werden später besprochen. Wichtig ist, daß der sachgerechte Umgang mit den Patientendaten durch Schutzmaßnahmen nicht beeinträchtigt werden darf – sonst werden sie bald mißachtet. Die Verfügbarkeit der Daten, besonders in kritischen Situationen, ist in jedem Fall oberstes Gebot. Und die Patientendaten müssen stimmen, damit der Arzt sich auf sie verlassen kann.

Der elektronische Patientenausweis

In diesem Jahr hat auch in Deutschland das Zeitalter der Chipkarte in der Medizin begonnen. In Hessen wird gerade in einem „Feldversuch“ der elektronische Patientenausweis für Kassenpatienten eingeführt. Noch enthält er nur die Identitätsdaten des Patienten und der Krankenkasse; er ersetzt also den Krankenschein. Angedacht ist aber auch die Aufnahme von Risikodaten (Allergien, Risikofaktoren, Unverträglichkeiten, weiterhin auch Impfpaß, Organspender-Ausweis, Röntgenpaß), schließlich mit der Zunahme der Speicherkapazität auch Behandlungsdaten bis hin zur kompletten Krankheitsgeschichte.

Neben den offensichtlichen Vorteilen bringt diese Karte aber auch eine Reihe von Problemen und Gefahren mit sich. Wie sieht es mit den Zugriffsrechten und dem Zugriffsschutz aus? Auch die perfekteste Sicherheitstechnik auf der Karte schützt nicht stärker als die PIN, die den Zugriff eröffnet. Wenn nur der Patient mit seiner PIN die Karte aktivieren kann: Was passiert im Notfall, wenn der Patient nicht handlungsfähig ist und seine Risikodaten besonders gebraucht werden? Was macht der Patient, in Zwangslagen, etwa

wenn ein Arbeitgeber Druck ausübt – er weiß ja, daß auf der Karte alles steht, und könnte die Offenlegung verlangen. Ähnliche Situationen von Machtmißbrauch soll es ja auch heute in anderer Richtung schon geben; der Kampf um den Arbeitsplatz ist eben hart. Wie sieht es mit der Zuverlässigkeit der Datenspeicherung aus? Kann für den Fall der Zerstörung oder des Verlusts ein Backup vorgehalten werden? Wo? Unter wessen Verantwortung?

Beweiskraft elektronischer Dokumente

Dürfen wir elektronische Dokumenten trauen? Die Antwort ist zunächst ein klares „Nein!“.

Falsch: „Dieses Dokument wurde von einer elektronischen Datenverarbeitungsanlage erstellt und ist daher ohne Unterschrift gültig.“

Richtig: „. . . und ist daher ohne jede Beweiskraft.“

Elektronische Dokumente kann man fälschen, ohne Spuren zu hinterlassen. Auch Bilder werden heute oft elektronisch bearbeitet und sind nicht mehr beweissicher.

Welche Beweiskraft haben archivierte Patientendaten im Streitfall? Wie kann man die Kommunikation zwischen verschiedenen Institutionen der Krankenversorgung beweissicher gestalten? Woher weiß der Apotheker, daß ein Rezept auch wirklich vom Arzt ausgestellt wurde, und zwar genau so, wie es vorliegt?

1.2 Die Automatisierung der Behandlung

Immer wieder wird in der Presse von Unfällen und Katastrophen berichtet, die durch die Automatisierung von Vorgängen, vor allem durch Software-Fehler verursacht wurden. Zwei Schlagzeilen:

- „Amoklauf der Maschinen“ (Die Zeit)[7].
- „Die programmierte Katastrophe“ (Der Spiegel)[11].

Welchen Schaden verursachen Computer in der Medizin?

Software-Fehler

Programme, insbesondere große Software-Systeme, sind grundsätzlich fehlerbehaftet. Es gibt Fehler im Detail (falsche Anweisungen) und Fehler im Großen (im Zusammenwirken von Programmteilen). Auch ein korrektes Programm kann falsche Ergebnisse liefern, wenn Spezifikation und Entwurf Fehler enthalten; so können zum Beispiel durch Digitalisierung von Bilddaten Artefakte entstehen. Bilddaten werden oft wegen ihres riesigen Umfangs komprimiert. Da umkehrbare Kompressionsverfahren die Dateien nicht genügend verkleinern, werden auch Verfahren mit Informationsverlust angewendet; das bedeutet, daß „unwesentliche“ Bilddetails nicht wieder herstellbar sind. Können solche Verfahren für medizinische Bilder verantwortet werden? Welche Details sind unwesentlich?

Trotz intensiven Testens treten Fehler in nicht antizipierten Sondersituationen auf; ein Beispiel wird gleich vorgeführt. Hat der Benutzer n Eingaben mit jeweils mindestens 2 Möglichkeiten zu machen, kann das Programm in mindestens 2^n verschiedene Situationen geraten. Ein vollständiges Testen wird also schon bei mäßig großem n durch die „kombinatorische Explosion“ verhindert.

Immer wieder mal wird von Informatikern die Software-Krise ausgerufen, überwunden wird sie nie. Dennoch muß man bedenken, daß Menschen auch Fehler machen – vielleicht sogar mehr als die Maschinen, durch die sie ersetzt werden.

Expertensysteme

Um die Tücken von Expertensystemen, aber auch die allgemeine Schwierigkeit, Programme korrekt zu gestalten, zu zeigen, will ich ein „triviales“ Demonstrationsbeispiel aus einem gängigen Entwicklungssystem vorführen. Es geht nicht darum, ein bestimmtes Produkt schlecht zu machen, sondern nur darum, die Fallen bei der Entwicklung von Expertensystemen zu verdeutlichen. Das Beispiel selbst ist trivial und erhebt keinen Anspruch, ernstgenommen zu werden.

```
Hi. I am your animal identification system.
Please describe one of the following animals.
The animals that I have knowledge about are:

      albatross
```

penguin
ostrich
zebra
giraffe
tiger
cheetah

Animal appearance:
(Choose any number of the following:)

x___ has feathers
____ has fur
x___ has hooves
____ has long neck
____ has claws

What does animal's mother produce?
(Choose one of the following:)

x___ lays eggs
____ gives milk

How does the animal move about?
(Choose any number of the following:)

x___ flies
____ flies well
____ swims
____ runs or walks

Animal color and markings:
(Choose any number of the following:)

____ tawny
____ black stripes
____ dark spots
x___ black and white

```
-----------------------------------------------------

 The animal's identity is albatross.
-----------------------------------------------------
           ---- How ----
 I assigned value to the animal's identity of IDENTITY by

 1. Rule ALBATROSS1 which states that

 if ANIMAL CLASS is 'bird' and
 ANIMAL LOCOMOTION is ('flies','flies well')
 then there is 0.9 evidence that the animal's identity = 'albatross'.

 As a result of this rule
 the animal's identity has been assigned =
     'albatross' (.9).

 2. Rule ALBATROSS2 which states that

 if ANIMAL CLASS is 'bird' and
 ANIMAL LOCOMOTION is ('flies','flies well') and
 ANIMAL COLOR is 'black and white'
 then the animal's identity = 'albatross'.

 As a result of this rule
 the animal's identity has been assigned = 'albatross' (1).
```

Ergebnis: Das Expertensystem hat in einer unvorhergesehenen Situation (es sollte einen Flugdrachen identifizieren) eine Angabe („hat Hufe“) einfach ignoriert und einen Fehlschluß gezogen.

Dieses Verhalten ist typisch für Expertensysteme: Die Extrapolation über den Rand des erfaßten Bereichs hinaus ergibt oft falsche Ergebnisse. Insbesondere regelbasierte Systeme führen schon bei mäßigem Umfang zu verschlungenen „Regelspaghetti“, die eine Korrektheitsüberprüfung kaum noch möglich erscheinen lassen. Warum haben die Entwickler den Fehler im Beispiel nicht entdeckt? Es gibt 14 verschiedene Ja-nein-Eingaben. Ein vollständiger Test dieses (lächerlich kleinen) Sytems müßte 2^{14}, also über 16000 verschiedene Situationen umfassen.

Sollen Expertensysteme in der medizinischen Praxis angewendet werden, so ist zum mindesten eine Evaluation analog zu anderen Therapiehilfen (Me-

dikamente, Geräte, ...) nötig. Menschliche Experten sind nicht ersetzbar. Dennoch zeichnen sich zwei neue Arten von ärztlichen Kunstfehlern ab: der Einsatz eines Expertensystems und der Nichteinsatz eines Expertensystems.

Software-Erstellung

Oft ist mangelnde Professionalität bei der Erstellung medizinischer Programme zu beklagen, insbesondere bei Endbenutzer-Programmierung. Methoden der Qualitätssicherung (Tests, Verifikationsmethoden) werden gar nicht oder nur mangelhaft angewendet. Als anderes Extrem gibt es nichtmedizinische Informatik-Profis mit sicherheitskritischen Funktionen, die kein Verständnis für resultierende medizinische Gefahren haben. Eine besondere Gefahr bedeutet die sich abzeichnende universelle Verwendung der Programmiersprache C mit ihren mangelhaften Sicherheitsstandards; auch erfahrenen Programmierern unterlaufen immer wieder die gleichen gefürchteten Fehler. So wurden bei einem systematischen Test von UNIX-Systemsoftware ungefähr 25% aller untersuchten Dienstprogramme als fehlerhaft entlarvt; die Fehler ließen sich hauptsächlich auf typische C-Fehler zurückführen [8].

Benutzer-Führung

Der weitaus häufigste Grund für Datenverlust sind Fehler durch Unwissenheit oder Nachlässigkeit; niemand schützt den Benutzer vor sich selbst. So kann eine Datei zerstört werden, wenn der Benutzer den PC abschaltet, während sie noch offen ist. Eine neue Variante: Abschalten bei Multitasking in Windows mit 15 laufenden Programmen. Auch moderne „benutzerfreundliche“ Fenstersysteme sind keine Garantie gegen Bedienungsfehler. Gefährlich ist der Eintrag von Daten in das falsche von 22 offenen Fenstern. Man stelle sich vor, daß ein Arzt mehrere Patientenakten gleichzetig geöffnet hat und sich in der Eile vertut.

1.3 Schwachstellen im PC-Betrieb

Ich will an ein paar Beispielen deutlich machen, wie „offen“ und verletzbar PCs sind. Hardware und Betriebssystem sind offen bis zum letzten Bit konzipiert. Das hat fatale Konsequenzen für die Sicherheit. Im Bereich der Workstations unter UNIX ist die Situation durch den dort üblichen Paßwortschutz etwas besser, aber viele der folgenden Kritikpunkte treffen auch hier

zu.

Grundsätzliche Mängel

Beispiel 1: *Mangelnde Funktionstrennung.* Es gibt keine Funktionstrennung von Systemverwaltung, Bedienung, Programmierung und Anwendung. Der Anwender ist Auftraggeber, Programmierer, Operator, Archivar, ... in einer Person und kann mit seinem PC und den darauf gespeicherten Daten alles machen – absichtlich oder aus Versehen.

Beispiel 2: *Kein physischer Schutz.* Ein wirksamer physischer Schutz ist im Vergleich zu den geringen Gerätekosten vergleichsweise teuer und daher nicht wirtschaftlich.

Beispiel 3: *Die Geräte sind wegtragbar.* Und oft sind sie unbewacht. Ein Angreifer, der einen PC samt Festplatte geklaut hat, hat dann sehr viel Zeit, um vorhandene Schutzmechanismen zu studieren und zu knacken.

Beispiel 4: *Datendiebstahl.* Daten sind leicht auf Disketten zu kopieren und unauffällig wegtransportierbar. Im Gegensatz zum Diebstahl der Brieftasche merkt der Besitzer den Diebstahl von Daten nicht.

Beispiel 5: *Systemkenntnisse.* Gute Systemkenntnisse sind bei möglichen Angreifern weit verbreitet. 'Security by obscurity' kann nicht funktionieren.

Beispiel 6: *Das Bananenprinzip.* Software wird meist unreif, das heißt, fehlerbehaftet, ausgeliefert und „reift beim Kunden". Hoffentlich werden nicht durch Fehler wichtige Daten beschädigt.

Datenträger

Beispiel 1: *Alle Daten sind lesbar.* Jeder, der einen PC bedient, kann alle auf ihm gespeicherten Daten sehen. Auch wenn diese von einem Datenbanksystem in speziellem Format abgespeichert und innerhalb der zugehörigen Anwendung etwa durch ein Paßwort geschützt sind, kann die halbwegs geübte Benutzerin von der Betriebssystemebene aus sogar mit einem einfachen Editor oder dem TYPE-Kommando vieles sehen, was sie eigentlich nicht darf. Fast genau so leicht kann sie die Daten auch ändern.

Beispiel 2: *Die Festplatte muß zur Reparatur.* Stellen Sie sich vor, Sie haben Patientendaten auf der PC-Festplatte gespeichert. Durch einen Fehler funktioniert die Festplatte nicht mehr – vielleicht muß ein Chip in der Plattensteuerung ausgetauscht werden. Die Platte mit allen Daten wandert zur Reparatur. Der Techniker kann sie in Ruhe lesen. In der Regel wird er das

nicht tun. Aber die Hoffnung darauf ist keine ausreichende Datenschutzmaßnahme.

Beispiel 3: *Vernichten von Disketten.* Eine Diskette oder Festplatte ist nicht mehr brauchbar. Zum Löschen der Daten ist es zu spät – nichts geht mehr. Sie werfen sie weg (selbstverständlich zum Recycling). Wissen Sie, welche Datenreste noch vorhanden sind? Es gibt Spezialgeräte zur Datenrettung, mit denen man auch auf beschädigten Datenträgern noch ziemlich viel lesen kann, auch Datenreste in 'bad sectors'. Vielleicht wühlt ein Journalist im Müll der Klinik, um die Datenschutzmaßnahmen zu diskreditieren?

Beispiel 4: *Löschen von Dateien.* Gelöschte Dateien sind nur im Verzeichnis als gelöscht markiert. In Wirklichkeit stehen die Daten noch da, bis sie irgendwann von anderen Schreibvorgängen überschrieben werden. Bei Festplatten (im Gegensatz zu Disketten) werden die Daten nicht einmal beim gewöhnlichen Formatieren gelöscht. Mit einem Disketten-Monitor wie etwa den „Norton Utilities" kann man diese Daten leicht sehen, oft sogar ganze gelöschte Dateien wiederherstellen. Besonders kritisch ist, daß viele Programme, auch Verschlüsselungsprogramme, temporäre Dateien anlegen und diese ungenügend löschen; ähnlich ist es mit virtuellem Speicher (dem Swapfile von Windows). Aus der Werbung:

> Wir können Ihre verlorenen Daten wiederherstellen. Egal ob Ihre Festplatte defekt ist, Sie Ihre Daten aus Versehen gelöscht haben oder eine andere Art von Zugriffsproblem Ihren Betrieb lähmt – $***$ kann bei Datenverlust Wunder wirken. ... Unsere Erfolgsrate beträgt 95%. ...

Beispiel 5: *Müll am Dateiende.* Vielleicht wissen Sie, daß das Betriebssystem MS-DOS bzw. PC-DOS bei Schreibvorgängen den freien Raum hinter dem Ende einer Datei bis zum Ende des Sektors mit Daten vollschreibt, die zufällig in einem internen Puffer stehen – das können durchaus Daten sein, die Sie eigentlich geheimhalten wollten, siehe Abbildung 1. Nicht benötigte Sektoren im Cluster behalten ihren alten Inhalt. Auch diese Daten kann man mit einem Disketten-Monitor leicht sehen.

Hardware und Schnittstellen

Beispiel 1: *Anschlüsse auf der PC-Rückseite.* Viele Daten lassen sich über die Standard-Schnittstellen abgreifen. So bietet es sich auf diskettenlosen Arbeitsplätzen als Ersatz an, die Daten auf den Druckerausgang umzulenken. Auch die Hardcopy-Taste ('PrtSc') kann zu diesem Zweck dienen, und ihre Verwendung ist kaum zu kontrollieren.

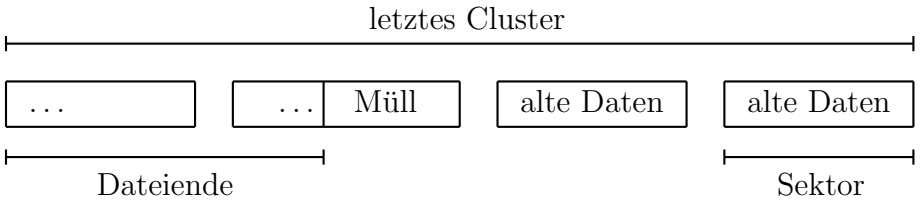

Abbildung 1: Datenmüll am Dateiende

Beispiel 2: *Systembus.* Das Innenleben eines PCs ist leicht zugänglich. Zum Beispiel lassen sich leicht Abhöreinrichtungen („Wanzen“) auf Lötkontakte klemmen, mit denen man Paß- und Schlüsselwörter abhören und danach jeden Softwareschutz unterlaufen kann. (Denken Sie auch an den Wartungsdienst – wer hat schon die Zeit, einem Techniker beim Austausch einer Festplatte eine halbe Stunde lang auf die Finger zu schauen.)

Beispiel 3: *SCSI-Bus.* Eine elegante Möglichkeit zum Anschluß externer Festplatten, Streamer, optischer Laufwerke. Leider liegt der ganze Datenverkehr von und zu diesen Geräten buchstäblich im Freien.

Beispiel 4: *Tastatur.* Ist die Zentraleinheit nicht so leicht zu öffnen, kann man auch Abhörgeräte in die Tastatur einbauen. Zumindest ein Paßwort wird dabei doch wohl herausspringen. Auch läßt sich die Wirkung der Tasten manipulieren.

Beispiel 5: *Monitor-Abstrahlung.* Es wurde schon wiederholt im Fachzeitschriften beschrieben und sogar im Fernsehen gezeigt, wie leicht man mit einer vergleichsweise primitiven Ausrüstung noch in größerer Entfernung das Geschehen auf einem Bildschirm duplizieren kann.

Beispiel 6: *Booten von Diskette.* Viele Schutzmaßnahmen auf der Festplatte, so etwa das DRDOS-Paßwort, kann man umgehen, indem man einfach eine Systemdiskette einlegt und den Dreifingergriff anwendet. (Das reicht bei DRDOS noch nicht ganz, aber siehe Beispiel 8.) Ein Zitat aus der Netnews-Gruppe ‘comp.security.misc’ (empfangbar für jeden, der einen Internet-Anschluß hat): „Es hält den ernsthaften Cracker 122 Minuten auf (2 Stunden, um mit den Lachkrämpfen fertig zu werden, und zwei Minuten, um den Schutz zu umgehen.)“ (Übersetzung von mir.)

Beispiel 7: *Hardware-Paßwort.* Mache PCs oder Workstations haben ein Hardware-Paßwort im BIOS-Setup, mit dem man gewisse Konfigurationsmerkmale schützen kann, z. B. das Boot-Laufwerk. Das Paßwort wird gelöscht, indem man die Batterie herausnimmt. Hilft das nichts, kann man auch das ROM austauschen.

Beispiel 8: *ROM-Monitor mit Zugriff auf Festplatte.* PCs haben ein Monitor-Programm im ROM, mit dem man eine physikalisch angeschlossene Festplatte Sektor für Sektor untersuchen und eventuelle Schutz-Bytes ändern kann, zumindest, wenn sie einen Standard-BIOS-Treiber hat.

Sabotageprogramme

Siehe den Vortrag über Viren.

Trügerische Sicherheit

Beispiel 1: *Standard-Anwendungen.* Zitat aus dem Handbuch des bekannten Verschlüsselungsprogramms 'pgp': „Es gibt eine Firma namens ∗∗∗, die für $185 ein Programmpaket vertreibt, das die eingebauten Verschlüsselungsverfahren von WordPerfect, Lotus 1-2-3, MS Excel, Symphony, Quattro Pro, Paradox und MS Word knackt. ... Der Autor sagte, man brauche nur den Bruchteil einer Sekunde zum Knacken, aber er habe einige Verzögerungsschleifen eingebaut, damit es für den Kunden nicht zu leicht aussieht." Es gibt auch Public-Domain-Programme mit demselben Zweck. Einziger Trost: Ein vergessenes Paßwort ist überhaupt kein Problem.

Beispiel 2: *Schlechte Verschlüsselungsverfahren.* Nicht nur Standard-Programme, auch auf dem Markt vertriebene PC-Sicherheitssysteme verwenden z. T. schwache Verfahren [11]. Achtung: Aus den USA importierte Verfahren sind in der Regel schwach wegen der dortigen Export-Beschränkungen.

Beispiel 3: *Schutzvorkehrungen auf Servern.* Fred Cohen gab unlängst erste Ergebnisse eines systematischen Tests von Novell-Servern und UNIX-pcnfs-Servern bekannt. Es stellte sich heraus, daß viele Schutzbits gar nicht wirken; insbesondere konnten Viren auch 'execute only'-Dateien infizieren. Siehe [10, 13.74 und 13.76].

1.4 Netze

Medizinische Systeme werden immer mehr vernetzt. In Krankenhausabteilungen oder Arztpraxen werden lokale Netze installiert, in Krankenhäusern kliniksweite Backbone-Netze. Auch Zugriffe zu externen Informationsdiensten werden immer beliebter. Schließlich spricht man schon von Telemedizin – der Kommunikation zwischen medizinischen Systemen über Fernverkehrsnetze.

Kliniksnetze

Die Anforderungen von Patientenversorgung und Wissenschaft kollidieren. Die Patientenversorgung erfordert wegen des Datenschutzes ein Abschottung nach außen; ein wissenschaftlicher Arbeitsplatz benötigt aber den Anschluß ans Wissenschaftsnetz unt Internet. Auch externe kommerzielle Informationsdienste wie DIMDI sollten erreichbar sein. Nun ist das Internet weltweit offen für Hackerangriffe. Ein einziges schlechtes Paßwort genügt, um in ein System einzudringen und dort Unfug zu stiften. Firewall-Konzepte, die den Zugang in die weite Welt des Internet kontrollieren sollen, können durch ISDN-Anschlüsse (oder Modems) leicht umgangen werden.

Abhören von Netzen

Netze aller Art bieten Abhörmöglichkeiten auf allen Ebenen, mit denen man nicht nur lauschen, sondern zum Teil auch fälschen kann:

- Elektromagnetische Abstrahlung oder Induktion („Nebensprecheffekt“). Spezielle Geräte dafür kann man auf dem Markt kaufen oder als Elektronik-Bastler leicht selbst herstellen.
- Anzapfen der Leitung (‘wire tapping’). Bei Glasfaserkabeln ist das etwas schwieriger, aber auch möglich durch Abzweigen eines Teil-Lichtstroms.
- Anzapfen spezieller Kommunikationseinrichtungen wie Modems, Knotenrechner, Brücken (die im übrigen auch elektromagnetisch abstrahlen).
- Schnittstellen (Stecker raus, Schnittstellentester dazwischen, Stecker wieder rein).
- Spezielle Netzanalyse-Geräte (‘Sniffer’), die eigentlich für die Netz-Verwaltung da sind.
- Besetzung unbenutzter Anschlußpunkte oder Austausch eines gesicherten Systems durch ein ungesichertes. Oder Verbindung eines Laptops mit einem Netz-PC über die parallelen Schnittstellen mit einem Produkt wie ’lap2lan’.
- Manipulation regulärer Anschlüsse; denn lokale Netze sind „Diffusionsnetze“ – der gesamte Datenstrom läuft durch jede Station. Man braucht

nur die geeignete Software, um ihn zu analysieren, etwa Paßwörter herauszufiltern.

In solchen offenen Systemen muß man immer mit dem Zugriff durch Unbefugte rechnen. Auch Viren und andere Schadprogramme können leicht eindringen und sich ausbreiten.

1.5 Krankheitsregister

Krankheitsregister sind Datensammlungen zu epidemiologischen Forschungszwecken. Zur Zeit werden in allen Bundesländern Krebsregister vorbereitet. Große Datensammlungen dieser Art sind unter dem Aspekt des Datenschutzes besonders problematisch. Durch Abgleich mit anderen Datenbanken lassen sich, wenn keine besonderen Vorkehrungen getroffen werden, mühelos geballte Informationen über beliebige Bürger zusammenstellen. Eine möglichst gute Anonymisierung ist für Register also oberstes Gebot. Das allein reicht aber nicht. Es ist bekannt, daß weder die Einschränkung der Abfragemöglichkeiten noch die Anonymisierung für solche Datensammlungen echte Sicherheit bringen, wenn die Daten noch für irgendwelche Zwecke gut sein sollen [13, S. 156–170].

2 Sicherheitskonzepte für die Medizin-Informatik

Nach so vielem Reden über Probleme und Gefahren jetzt zur positiven Seite. Wie kann man medizinische Anwendungssysteme sichern und schützen? Sicherzustellen sind dabei Verfügbarkeit, Korrektheit und Vertraulichkeit der Daten, „wirksame“ Anonymisierung wo nötig, ferner Korrektheit, Integrität und softwaretechnische Qualität der Programme. Wesentliche Grundprinzipien, die im folgenden immer wieder durchscheinen, sind:

- Redundanz,
- physischer Schutz,
- Perfektion,
- Fehlertoleranz,
- Verschlüsselung,

- kryptographische Protokolle.

2.1 Offene und geschlossene Systeme

Die Definition der Begriffe „offen“ und „geschlossen“ vom sicherheitstechnischen Standpunkt:

geschlossenes System: Auf jeder Ebene wird wirksam und zuverlässig verhindert, daß Unbefugte am System manipulieren können. Es ist alles verboten und auch unmöglich, was nicht ausdrücklich erlaubt ist. Es herrscht das Prinzip der minimalen Rechte (‘need to know’) und der minimalen Schnittstellen.

offenes System: Manipulationen sind nicht lückenlos zu verhindern. Es ist alles erlaubt, was nicht ausdrücklich verboten ist, und möglich ist sogar einiges mehr.

Das Sicherheitsschalenmodell

Wie in einem geschlossenen System die Daten geschützt werden, läßt sich am einfachsten durch ein Schalenmodell verdeutlichen, siehe Abbildung 2.

Ist eine der äußeren Schalen durchlässig, so läßt sich der Schutz der inneren Schalen umgehen, das System ist nicht mehr geschlossen. Stahltüren in Pappwänden nützen nicht viel. Das verdeutlichen die Beispiele:

1. Die physische Sicherheit, die ein abschließbarer Raum bietet, nützt nichts ohne organisatorische Sicherheit – wenn sich niemand für das Abschließen zuständig fühlt.

2. Die Hardware-Sicherheit durch ein Schloß am PC nützt nichts ohne physische Sicherheit: Ein Dieb kann den PC einfach wegtragen und zu Hause in aller Ruhe aufbrechen.

3. Die Betriebssystem-Sicherheit eines Paßwortschutzes für die Festplatte nützt nichts ohne eine Hardwaresicherung, die das „Booten“ von einer Diskette verhindert.

4. Die Anwendungs-Sicherheit durch Vergabe von Zugriffsrechten in einem Datenbanksystem nützt nichts, wenn das Betriebssystem gestattet, die Festplatte sektorenweise zu analysieren.

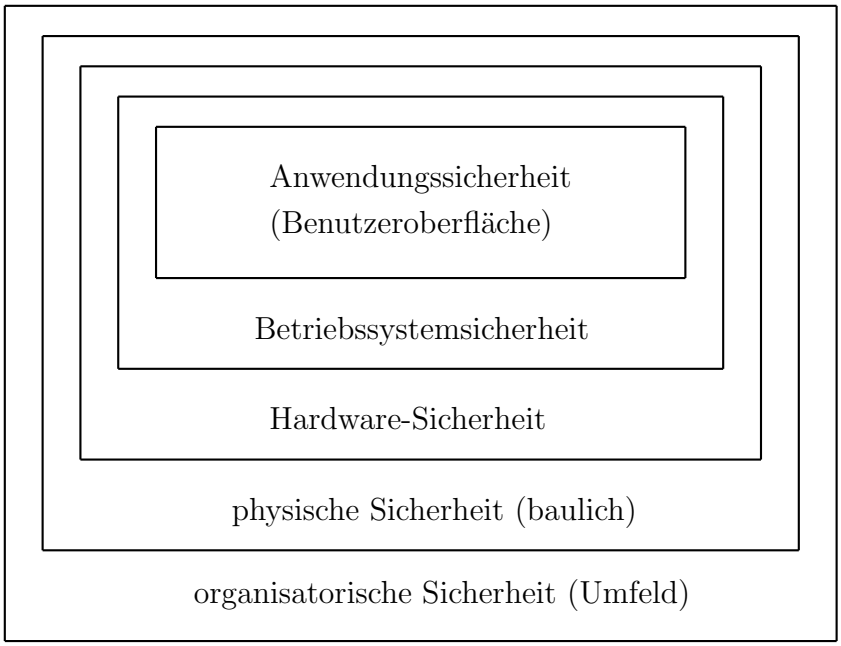

Abbildung 2: Die Sicherheitsschalen eines geschlossenen Systems

In einem geschlossen System reicht es tatsächlich, Zugriffsrechte auf bestimmte Daten durch Einträge in System-Tabellen zu definieren – das ist eine sichere Maßnahme. Die wichtigen Systemkomponenten sind physisch geschützt; auf dieser Grundlage lassen sich logischer Zugang zum System und Zugriff auf Daten wirksam durch das Betriebssystem und die Anwendungsprogramme überwachen. Dieser Schutz ist seit den 70er Jahren typisch für eine Großrechner-Umgebung ('closed shop').

Sicherheitsanforderungen in offenen Systemen

In den DFG-Richtlinien zur Rechnerbeschaffung werden offene Systeme empfohlen – auch für Universitätskliniken. Aber kann man offene Systeme in der Medizin überhaupt vertreten? Ist offen = unsicher, geschlossen = sicher? Das ist nicht notwendig so. Offenheit im systemtechnischen Sinne (meist als vernetztes System auf der Basis UNIX oder MSDOS verstanden) fördert zwar die sicherheitstechnische Offenheit, ist aber nicht notwendig mit ihr identisch. Einige Prinzipien, um den Konflikt „offen versus sicher“ zu bewältigen, sind:

- Sensible Daten in einem offenen System dürfen außerhalb der zugehöri-

gen Anwendungsprogramme nicht lesbar sein. Das wird durch *Verschlüsselung* erreicht.

- Der Datenzugriff innerhalb eines Anwendungsprogramms ist durch eine *Berechtigungsmatrix* zu regeln. Gleiches gilt für Datenzugriffe auf Server.
- Wichtige Daten müssen manipulationssicher *signiert* werden können. Auch dafür gibt es kryptographische Methoden.

Kryptographie („Geheimschrift“) ist die Lehre von der Datensicherheit in unsicheren Umgebungen, insbesondere in offenen Systemen. Sie bietet Lösungsansätze für die meisten Sicherheitsprobleme, manchmal sogar Patentlösungen. Die Umsetzung dieser Lösungen in die Praxis erfordert aber Sorgfalt und Augenmaß.

2.2 Vorbeugen von Fehlern

Die wichtigsten Sicherheitsmaßnahmen sind das Vermeiden oder Abfangen von Fehlern – oder die möglichst problemlose Rekonvaleszenz des Systems nach Fehlern.

Datensicherung

Das allerwichtigste für fast jeden Rechnerbetrieb ist die Sicherstellung der Verfügbarkeit der Daten. Dazu braucht man in erster Linie Backups, Backups, Backups. Sie tragen auch zum Schutz der Integrität der Daten und des Systems bei, da man den Zustand vor einer Verfälschung oder Manipulation wieder herstellen kann. Backupmedien gehören in den Safe.

Perfektion und Fehlertoleranz

Die beiden Prinzipien zur Fehlervorbeugung beim Entwurf von sicherheitskritischen Systemen sind Perfektion und Fehlertoleranz [6]. Beides sind Ideale, die nie erreicht werden, aber bestmöglich angestrebt werden sollen.

Perfektion bedeutet den Versuch, Fehler zu vermeiden. Die Methoden dazu sind ein sorgfältiger Entwurf bis hin zum Einsatz formaler Methoden und Fehlerelimination durch ausgiebige Tests.

Fehlertoleranz bedeutet den Versuch, die Auswirkung möglicher Fehler zu beschränken. Das geschieht durch den Einbau von Redundanz und Fehler-Abfangprozeduren.

Benutzerführung

Einige Punkte, die für eine möglichst sichere Führung der Benutzer durch Programme wichtig sind:

- Eine einheitliche, konsistente Benutzungsoberfläche.
- Intuitive Bedienung.
- Gestaltung der Software nach ergonomischen Anforderungen.
- Geschlossene Benutzungsoberfläche, d. h., der Benutzer kann in jedem Zeitpunkt nur eine Aktion aus einem übersichtlichen Angebot ausführen.
- Schutz vor Fehlbedienung.
- Eingabe mit Plausibilitätsprüfung.
- Kontextsensitivität.
- Individualisierung der Benutzung (persönliche Konfiguration).
- aufgabenbezogenes Benutzerprofil, abhängig vom Erfahrungshorizont ('expert level')
- Erkenntnisse der Fehlerpsychologie.

2.3 Kryptographische Techniken

Der Mangel an physischer Sicherheit in offenen Systemen kann durch kryptographische Maßnahmen, also Verschlüsselungstechniken, ausgeglichen werden, in mancher Hinsicht sogar verbessert (allerdings schützt Kryptographie nicht vor Vandalismus). Ohne Verschlüsselung ist echter Datenschutz auf dem PC und in Netzen nicht möglich. Die grundlegenden Techniken, Verschlüsselungsverfahren, elektronische Unterschrift und andere kryptographische Protokolle werden in einem späteren Vortrag behandelt.

Verschlüsselung von Dateien

Für den Zeitpunkt der Verschlüsselung der Daten auf der Festplatte gibt es zwei Konzepte: Das einfachere ist, daß Dateien vor der Bearbeitung entschlüsselt und nach der Bearbeitung wieder verschlüsselt werden. Das behindert bei der eigentlichen Arbeit dann zwar nicht mehr, muß aber in der Regel von Hand ausgeführt werden, so daß sich der Arbeitsbeginn verzögert, und am Ende steht die Gefahr, daß unerwünschte Datenreste auf der Platte bleiben oder daß man gar das Wiederverschlüsseln vergißt. Eine andere Lösung ist, daß die Daten während der Bearbeitung, also auf dem Weg zwischen Platte und Hauptspeicher ent- oder verschlüsselt werden ('online'); für 'online'-Verschlüsselung muß das Verfahren in einem Gerätetreiber installiert sein. Die Verschlüsselung ist zeitraubend, wenn sie per Software realisiert wird – und gerade die wichtigen Daten sind die, die man ständig braucht. Wird es dagegen per Hardware erledigt, ist es teuer. Auch sind nicht alle auf dem Markt angebotenen Verschlüsselungsverfahren so einbruchsicher, wie es die Werbung verheißt [11]. Dazu kommt, daß man sich ein Schlüsselwort merken muß (sonst taugt das Verschlüsselungsverfahren garantiert nichts), und damit beginnen die leidigen Paßwortprobleme.

Trotz aller Vorbehalte können auch einfache Verschlüsselungsprogramme nützlich sein, wenn man nicht mit professionellen Angreifern rechnen muß. Sie verhindern, daß geschützte Daten versehentlich offengelegt werden, etwa wenn eine Diskette auf dem Transport verloren geht. Auch die Festplatte eines PCs kann im Falle eines Hardware-Diebstahls so durchaus ausreichend geschützt sein.

Datenbanken

Eine ausreichende Grundsicherheit für ein Datenbanksystem, die auch auf Betriebssystemebene wirksam ist, kann nur durch verschlüsselten Plattenzugriff erreicht werden. Verschiedene Ansätze sind dafür denkbar:

- Ein kryptographischer Gerätetreiber, der unterhalb des Datenbanksystems angeordnet ist.
- Verschlüsselung in den Basis-I/O-Funktionen des Datenbanksystems. Das müßte vom Hersteller mitgeliefert werden oder erfordert Zugriff auf den Quellcode.
- Datenfeldverschlüsselung. Das ist ein gängiges Konzept, behindert aber

die Datenbankfunktionalität (z. B. Suche nach Zahlen in einem bestimmten Bereich).

Auf jeden Fall muß sich die nötige Schlüsselverwaltung in ein Anwendungsprogramm integrieren lassen. Die interne Zugriffsregelung auf Daten läßt sich dann durch eine Berechtigungsmatrix umsetzen.

Netze

Auch der Schutz von Netzen beruht neben allgemeinen Maßnahmen wie physischem Schutz und Netzmanagement wesentlich auf Kryptographie, nämlich auf Verschlüsselung und kryptographischen Protokollen auf verschiedenen Ebenen.

2.4 Allgemeine Sicherheitsmaßnahmen

PC-Sicherheitssysteme

Es gibt eine Reihe von fertigen Sicherheitsprodukten auf dem Markt, die je nach organisatorischer Umgebung, physischen Schutzmöglichkeiten und Schutzbedürftigkeit der Daten die Datensicherheit auf einem PC wesentlich verbessern können und ein beträchtliches Sicherheitsniveau ermöglichen. Gute Produkte kosten einiges an Geld und einige Mühe für die Einarbeitung und laufende Verwaltung. Sie bestehen teils aus Hardwarekomponenten, teils aus Software; am sichersten ist die Kombination von beidem. Ein Katalog von erwünschten Leistungsmerkmalen für PC-Sicherheitssysteme:

- Individuelle Anpassung an eine ausreichende Zahl von Benutzern.
- Individuelle Zuteilung von Programmen und Dateien.
- Anmeldung mit Namen und Paßwort, besser mit zusätzlicher Chipkarte. Alarm und Sanktionen nach einer einstellbaren Anzahl von Fehlversuchen.
- Leistungsfähige Paßwortverwaltung, die aber das Merken von Paßwörtern nicht zur Qual für den Benutzer macht.
- Geschlossene Benutzungsoberfläche (lückenlose Menüsteuerung), Sperre von DOS-Befehlen.

- Verschlüsselung nach einem anerkannten Verfahren.
- Sperren, Schreibschützen und Verstecken von Dateien.
- Sperre von Diskettenlaufwerken und anderen Peripheriegeräten und Anschlüssen.
- Bootschutz.
- Bildschirmabdunklung in Arbeitspausen.
- Beweissichere Aufzeichnung von Vorgängen (Log-Datei).
- Keine Manipulation von EXE-, COM-, BAT- oder SYS-Dateien.

Der PC wird damit (sicherheitstechnisch) zum geschlossenen System.

Sicherheitshardware

In die Kategorie Sicherheitshardware gehören abgeschirmte Terminals und Kommunikationsleitungen sowie einmal beschreibbare optische Platten ('WORM') zur manipulationsgeschützten Protokollierung von Vorgängen. Wechselbare Festplatten erlauben, auch größere Datenbestände sicher aufzubewahren, vorausgesetzt, man hat einen entsprechenden Safe. Andererseits haben Arbeitsplatzrechner ohne Diskettenlaufwerk in einem Netz den Vorteil, daß Daten nicht so leicht unbefugt wegtransportiert werden können. Außerdem lassen sich nicht so leicht Viren ins System kopieren. Das Umlenken von Ausgabedaten auf einen Drucker wird allerdings nicht verhindert. Eine Alternative zu diskettenlosen PCs sind Laufwerkschlösser.

Physischer Schutz

Viele Manipulations- und Zerstörungsmöglichkeiten werden unterbunden oder wesentlich erschwert, wenn die Zentraleinheit und die entfernbaren Datenträger physisch geschützt werden. Geignet dafür sind verschlossene Räume, Sicherheitsgehäuse, Datensafes.

Zugangssperren und Benutzerkontrolle

Die wichtigste, aber allein nicht ausreichende, Zugangssperre ist der Paßwortschutz. Zusätzlich zu empfehlen ist ein mechanischer Schlüssel oder ein

Kartenleser. Einfache Magnetkarten-Systeme bieten trotz recht hohen Preises in den meisten Anwendungsfällen keine ausreichende Sicherheit. Wer einen PC hat und zusätzlich etwa 5000 DM für ein Kartenlese- und -schreibsystem mit passender Software anlegt, kann Magnetkarten beliebig kopieren oder ändern. Deutlich erhöhte Sicherheit bieten dagegen Chip-Karten, die zusätzlich durch ein Paßwort („PIN“) geschützt sind. Ein anderes Konzept zur Zugangssperre sind Zahlenschlösser, „Hosentaschensender“, die den Rechner sperren, wenn ihr Träger sich entfernt, oder Dongles, die auf den Druckerport gesteckt werden und einen kryptographischen Schlüssel enthalten (am ehesten geeignet für tragbare Rechner).

Das Personal Secure Environment

Eine unangenehme Begleiterscheinung eines ausgefeilten Sicherheitskonzepts ist, daß der Benutzer mehrere komplizierte Schlüssel kennen muß; z. B. sind RSA-Schlüssel ganze Zahlen mit mindestens 200 Dezimalstellen. Das kann sich keiner merken. Daher braucht jeder Benutzer eine Schlüsselablage, das PSE (= Personal Secure Environment). Selbstverständlich ist es vor allen anderen Benutzern zu schützen, und das bedeutet, daß es selbst verschlüsselt sein muß. Der Schlüssel hierzu sollte aber leicht zu merken sein – eine PIN (= persönliche Identifikationsnummer) wie bei der Scheckkarte. Diese PIN ist alles, was sich der Benutzer merken muß; zur Erhöhung der Merkbarkeit ist es vorzuziehen, einen kurzen Satz als Paßwort zu verwenden, aus dem die eigentliche PIN vom Programm berechnet wird.

Wo wird nun dieses PSE aufbewahrt? Dazu gibt es drei Möglichkeiten mit zunehmender Sicherheit:

- eine Datei im System,
- eine persönliche Diskette,
- eine Chipkarte.

Die erste Art der Aufbewahrung ist schwach, da die PIN dann den ganzen Schutz darstellt. Bei den anderen Arten kommt als Schutz der persönliche Besitz eines Gegenstands hinzu. Die Chipkarte bietet darüber hinaus noch die bessere Fälschungssicherheit, da sie ihre eigenen Auswertungsprogramme enthält, und ermöglicht ‘Challenge-Response’-Mechanismen. Sie ist somit der ideale PSE-Träger.

Gegenstück des PSE ist ein öffentliches Verzeichnis der Prüfschlüssel, das vom Systemverwalter signiert wird. Und damit dieses wirklich vertrau-

enswürdig ist, verwahrt jeder Benutzer den Prüfschlüssel des Systemverwalters sicher auf: in seinem eigenen PSE. Durch diese Maßnahme wird das Signaturverfahren erst beweissicher. Der Systemverwalter ist somit eine absolute Vertrauensinstanz in diesem System.

Was steht nun alles im PSE? Alles, was der Benutzer wissen muß, aber sich nicht merken kann, und alles, worauf er sich verlassen muß:

- ein Kennwort, das zur Prüfung der korrekten Entschlüsselung und damit zur Verifikation des Schlüssels dient (etwa der Name der Anwendung),
- der Name des Besitzers,
- der Hauptschlüssel der Anwendung,
- der private Signaturschlüssel,
- der Prüfschlüssel des Systemverwalters.

2.5 Sicherheitskonzepte für medizinische Anwendungssysteme

Abteilungssystem und Arztpraxissystem

Ein sicheres Modell für ein klinisches Abteilungssystem oder ein Arztpraxissystem sollte etwa so aussehen: Für die gemeinsame Datenhaltung dient ein physisch geschützter Server. Soweit die Kommunikation über ungeschützte Leitungen verläuft, wird sie von der Netzsoftware automatisch verschlüsselt. Der Zugriff von Arbeitsplätzen auf den Server ist zeitlich geregelt, soweit sinnvoll. Außerdem sind Verschlüsselung und Signatur in die Anwendung eingebaut, PSE und PIN-Abfrage in Anwendung integriert. (Die Verschlüsselung innerhalb einer Anwendung ist von der Verbindungsverschlüsselung im Netz unabhängig.) Der Aufbau einer solchen Anwendung wird durch die Abbildung 3 anschaulich gemacht.

Während das Signaturverfahren problemlos in die Anwendung integriert werden kann, bietet die Verschlüsselung technische Probleme. Sie wird in einen Programmteil namens „kryptographischer Treiber“ gepackt, für den die Optionen im Abschnitt über Datenbanken genannt wurden. Beim Zukauf kommerzieller Lösungen ist zweierlei zu beachten: Das Verschlüsselungsverfahren muß ausreichend sicher sein – das ist bei vielen Produkten leider nicht

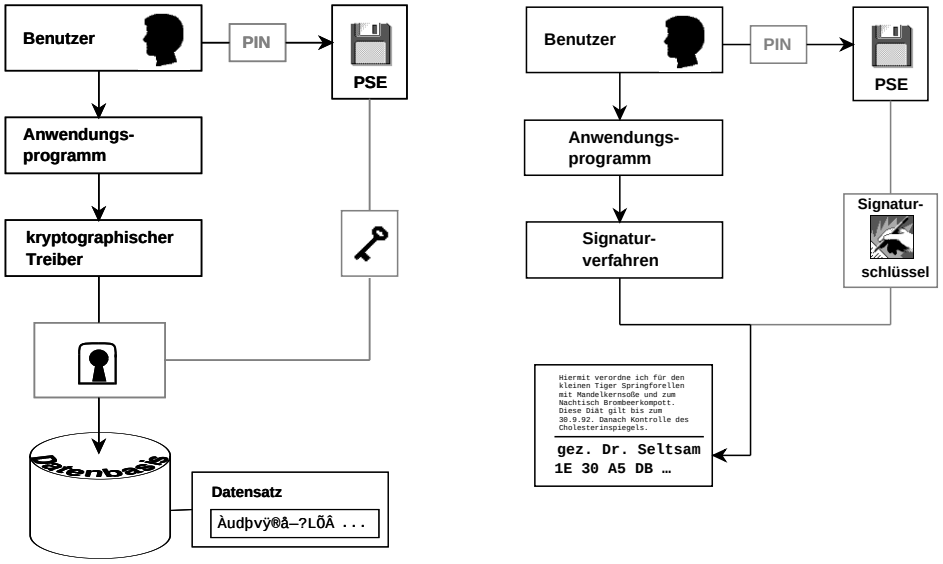

Abbildung 3: Das Sicherheitsschema für Datenschutz und Signatur

der Fall! Und die PIN-Abfrage muß sich in das Anwendungsprogramm integrieren lassen, damit nicht bei jedem Benutzerwechsel ein Programmneustart nötig wird.

Das Kliniksnetz

Forschung und Patientenversorgung müssen auf dem Kliniksnetz logisch oder physisch getrennt werden, oder man muß die Außenwelt strikt abkoppeln.

Eine physische Trennung bedeutet, daß zwei Kabel parallel geführt werden; das für ein solches Netz in der Regel Lichtwellenleiter verwendet werden, bedeutet es nur, daß die genügend vielen vorhandenen Fasern aufgeteilt werden. Der Nachteil ist, daß jede einzelne Netzstation strikt einem der beiden Netze zugeordnet werden muß. Ohne Übergänge geht es natürlich nicht; diese müssen dann durch Umstöpseln hergestellt werden.

Eine logische Trennung müßte auf einem geeigneten kryptographischen Protokoll beruhen, das für jeden Arbeitsplatz in jedem Zeitpunkt die Zuordnung zu einem der beiden Netze kennt. Auch der Übergang zwischen beiden Netzen ließe sich kontrolliert durch ein solches Protokoll regeln. Nachteil: Ein solches Protokoll hat noch niemand entwickelt, und die kryptographische Infrastruktur ist nicht vorhanden.

Eine Möglichkeit, ohne Trennung der Netze auszukommen, bietet das

Firewall-Konzept. Hier wird ein kontrollierter Zugang zur Außenwelt über einen dedizierten Rechner ermöglicht. Nachteil: Der Firewall-Rechner wird leicht zu einem Engpaß, und er kann verschiedene Systeme nicht optimal bedienen (z. B. eine Windows-Oberfläche eines externen Informationsdienstes durchreichen).

Der Datenverkehr auf dem Kliniksnetz sollte grundsätzlich nur verschlüsselt erfolgen; dazu sind in den (selbstverständlich physisch geschützten) Netzknoten kryptographische Einrichtungen unterzubringen.

Der Sicherheitsbeauftragte

Jede informationelle Einheit braucht einen hauptamtlichen Spezialisten (Informatiker oder besser Medizin-Informatiker), der für die Systembetreuung, insbesondere für die Datensicherheit, zuständig ist, und den gleichen Geheimhaltungsverpflichtungen unterliegt wie die anderen Mitarbeiter; er ist also Mitglied des „Behandlungsteams“. Natürlich muß auch ein Vertreter mit mindestens halber Arbeitszeit existieren (z. B. ein Mediziner mit Informatik-Kenntnissen). Bei kleineren Einheiten kann man auch an einen externen oder zentralen Dienst denken, aber das ist schon problematisch im Sinne der Datenschutz-Vorschriften; man sollte hierfür ein Modell mit einem geeigneten kryptographischen Protokoll entwickeln.

Unabhängig davon ist der Datenschutzbeauftragte der Klinik zu sehen, der eher ein Mediziner sein sollte.

Die Patientenkarte

Die Verfügung über die gespeicherten Daten sollte grundsätzlich beim Patienten liegen. Aber im Notfall müssen die Daten für einen Arzt mit einem „Universalschlüssel“ lesbar sein; dieser Vorgang ist manipulationssicher zu protokollieren (in Patientenkarte und Arztkarte). Alles dies ist durch geeignete kryptographische Protokolle sicherzustellen.

2.6 Sicherheitsstandards für medizinische Anwendungssysteme

Die IT-Sicherheitskriterien

... wurden in einem früheren Vortrag behandelt.

Sicherheitsstandards für medizinische Software

Aus den allgemeinen Sicherheitsstandards sind Standards für medizinische Anwendungssysteme herzuleiten. Software-Ersteller tragen hier eine besonders hohe Verantwortung. In der Analyse-Phase muß auch eine Risikoanalyse durchgeführt werden. Wo möglich, sind formale Methoden für Spezifikation, Design und Implementation anzuwenden. Test und Qualitätssicherung müssen dem Stand der Technik entsprechen, sowohl für die Komponenten als auch für die Integration der Komponenten ins Gesamtsystem. Zu fordern ist eine unabhängige Zertifikats-Instanz für lebenskritische Software. Über die Tests hinaus muß die Anwendung evaluiert werden: Es muß das Risiko des Einsatzes gegen das des Nichteinsatzes abgewogen und die Fehleranfälligkeit mit der des menschlichen Handelns verglichen werden. Hier sind Verfahren analog zur Arzneimittelprüfung nötig. Gefundene Fehler sollten nicht als Geheimsache behandelt, sondern in einem offenen Fehler-Reportsystem dokumentiert werden.

Sicherheitsstandards für medizinische Hardware

Neben der elektrischen Sicherheit nach der Medizin-Geräte-Verordnung muß auch die Störfestigkeit gegenüber elektromagnetischen Einstrahlungen sichergestellt werden. Die Methoden der klassischen Zuverlässigkeitstechnik [6] sind anzuwenden.

Krebsregister

Zur Gewährleistung des Datenschutzes sollten Datensätze in Krebsregistern nur anonymisiert gespeichert werden. Der Zugang zu diesen Daten darf trotzdem nur für angemeldete Forschungsvorhaben gewährt werden. In Ausnahmefällen ist eine Reidentifizierung von Datensätzen nötig.

Das Modell für das baden-württembergische Krebsregister sieht vor, daß die Daten beim behandelnden Arzt vor der Meldung asymmetrisch verschlüsselt werden. Die Reidentifikation ist dann nur über diesen Arzt möglich. Die Praktikabilität des Verfahrens und die erzielbare Datenqualität können bezweifelt werden. Für das Krebsregister Rheinland-Pfalz wurde daher unter

dem Leitgedanken *„hohe Datenqualität ohne Kompromittierung des Datenschutzes“* ein modifiziertes Registrierungsverfahren vorgeschlagen, das zwei wesentliche Schutzvorkehrungen enthält:

- die „informationelle Gewaltenteilung“ des Registers in eine Vertrauensstelle und eine Registerstelle; dazu kommt noch eine externe Stelle mit Sonderfunktionen;
- die Anonymisierung der Datensätze mit kontrollierter Abgleichmöglichkeit durch asymmetrische Verschlüsselung der Identitätsdaten und zusätzliche Bildung von Kontrollnummern.

Grundlage ist ein *Melderecht* des Arztes.

Die Vertrauensstelle steht unter ärztlicher Leitung, unterliegt also der Schweigepflicht. Sie verschlüsselt die Identifikationsmerkmale nach einem asymmetrischen Verfahren (faktische Anonymisierung). Der „öffentliche“ Schlüssel ist aber nur intern verfügbar und als Geheimnis der Vertrauensstelle zu behandeln. Der „private“ Schlüssel liegt beim externen Aufsichtsträger. Die Daten werden in der Vertrauensstelle nach einem „Zeitfenster“ gelöscht. **Die Registerstelle** erhält und speichert von jedem Datensatz

- die verschlüsselten Identitätsdaten,
- die Kontrollnummern,
- die epidemiologischen Daten.

Sie hat keinen Zugriff auf den „öffentlichen“ Schlüssel, d. h., sie kann keine „Probeverschlüsselung“ ausführen. Ein Zugriff auf Registerdaten wird nur für genehmigte Forschungsvorhaben gestattet. **Die externe Stelle** hält nur den „privaten“ Schlüssel und entschlüsselt in begründeten Ausnahmefällen einen Datensatz.

Die Kontrollnummern werden aus den Identitätsdaten durch Einweg-Verschlüsselung gewonnen, d. h., eine Entschlüsselung ist hier völlig unmöglich. Sie werden in der Vertrauensstelle gebildet und bei der Registerstelle zusammen mit dem zugehörigen Datensatz gespeichert. Die Kontrollnummern dienen zum Abgleich neuer Fälle mit bereits registrierten Fällen; dies wird zwar im Prinzip bereits durch die gespeicherten verschlüsselten Identitätsdaten ermöglicht, aber die Probleme der Homonyme und Synonyme erfordern zusätzliche Maßnahmen, um kleine Abweichungen in den Identitätsdaten durch Erfassungsfehler erkennen und korrigieren zu können und so die Datenqualität zu sichern.

Bei der Registerstelle werden die Kontrollnummern eines neu eingegangenen Falls mit den bereits gespeicherten Kontrollnummern (einschließlich

der verschlüsselten Identitätsdaten) abgeglichen. Bei Übereinstimmung des ganzen Satzes von Kontrollnummern werden die Fälle als identisch angesehen. Bei Abweichung, aber Übereinstimmung mindestens je einer Kontrollnummer, entsteht ein Verdacht auf Synonym. Dieser wird sofort nach Entdeckung an die Vertrauensstelle zurückgemeldet, die die Identitätsdaten noch im Klartext vorliegen hat und somit eine Klärung einleiten kann, ohne daß im Normalfall eine Entschlüsselung notwendig wird. In Ausnahmefällen wird allerdings eine Klärung nur nach Entschlüsselung der Identitätsdaten möglich sein. Auch bei speziellen Forschungsvorhaben kann eine Reidentifizierung von Datensätzen nötig sein, um weitere benötigte Daten zu erheben. Die Entschlüsselung der Identitätsdaten (in den erlaubten Fällen) ist nur der externen Stelle möglich.

3 Zusammenfassung

Sicherheit verursacht Kosten. Das können direkte Kosten für bauliche Maßnahmen oder zusätzliche Software sein oder Kosten für zusätzliches Personal mit Sicherheitsaufgaben. Kosten entstehen aber auch indirekt in Form von Zeit und Mühe. Zeit braucht man für die Planung, aber auch im täglichen Umgang mit den Sicherheitsmaßnahmen. Mühe verursachen die ständig geforderte Aufmerksamkeit oder lästige Identitätskontrollen. Nicht zu vergessen ist auch, daß einige Schutzmaßnahmen wie die Verschlüsselung oder die Überprüfung von Zugriffsberechtigungen auf Datenfeld-Ebene Datenverarbeitungsleistung kosten und die Antwortzeiten erhöhen. Andererseits sinken die Kosten für systeminterne Schutzmechanismen durch den Preisverfall der Hardware, der immer weiteren Verfügbarkeit von Standard-Software-Lösungen und der immer größeren Leistungsfähigkeit der Systeme, die einen Leistungsverlust durch Schutzmaßnahmen verschmerzbar macht. Und warum sollte man nicht einen kleinen Teil der Systemleistung eines modernen PCs, der für den Betrieb einer grafischen Benutzungsoberfläche draufgeht, für erhöhte Sicherheit opfern!

Bei der Abwägung von organisatorischen Maßnahmen statt eingebauter Schutzmechanismen ist zu bedenken, daß organisatorische Maßnahmen (z. B. Verbote) zwar oft wenig kosten, aber mit der wachsenden Komplexität der Systeme auch immer unübersichtlicher und schwerer zu überwachen werden und von der Zuverlässigkeit der Mitarbeiter abhängen. PC-Sicherheitssysteme zum Beispiel verlagern einen großen Teil der nötigen Disziplin von der Vielzahl der Endbenutzer auf den einen Sicherheitsexperten, der für die kompetente Auswahl sorgt, reduzieren die Schulungsnotwendig-

keit und verkürzen die lange Liste von Vorschriften „Sie dürfen nicht ..., Sie müssen ...“.

Medizin-Informatiker sind gefordert, Standards für die IT-Sicherheit in der Medizin zu entwickeln und vorzuschlagen, und zwar in Zusammenarbeit mit den Medizinern. Sicherheitsmaßnahmen müssen so konzipiert werden, daß sie den täglichen Ablauf in Klinik oder Praxis so wenig wie möglich behindern. Auch wenn perfekte Sicherheit nicht möglich ist, kann doch an vielen Stellen durch Automatisierung die Sicherheit erhöht werden, besonders wenn nicht an der menschlichen Überwachung der Prozesse gespart wird.

Und zum Schluß noch ein paar Merksätze:

- Vertrauen auf Unwissenheit ('security by obscurity') ist keine Datenschutzmaßnahme.
- Soweit möglich sollte man ein geschlossenes System anstreben, insbesondere für physischen Schutz sorgen.
- Daten lassen sich in offenen Systemen wirksam schützen, wenn, aber auch nur wenn, man kryptographische Methoden anwendet.
- PCs müssen, um den Anforderungen des Datenschutzes zu genügen, mit Sicherheitssystemen geschützt werden.
- Datenverkehr in Netzen sollte grundsätzlich verschlüsselt werden.
- Für medizinische Anwendungssysteme aller Arten sind geeignete technische Standards in Anlehnung an die IT-Sicherheitskriterien wünschenswert, die man den Herstellern gegenüber durchsetzen kann und die die Planung und Beurteilung von Systemen erleichtern. Insbesondere ist eine geeignete kryptographische Infrastruktur zu schaffen.
- Die technischen und organisatorischen Sicherheitsmaßnahmen in einer Klinik oder Praxis sind nicht nebenbei zu erledigen. Sie erfordern eine klare Festlegung der Verantwortlichkeiten und die Einplanung eines angemessenen Zeitaufwands. Durch Sicherheitsstandards läßt sich das Ausmaß der nötigen technischen Kenntnisse reduzieren; die Schulung und Pflege des Sicherheitsbewußtsein fordert dann aber immer noch einigen Aufwand.

Literatur

[1] H. Bassen et al.: Computerized medical devices. In: *Proc. 7th Annual Conference of IEEE Engineering in Medicine and Biology Society*, Chicago, Sept. 27–30, 1985, pp. 180–185.

[2] Albrecht Beutelspacher: *Kryptologie.* Vieweg, Braunschweig 1987.

[3] Jonathan Bowen, Victoria Stavridou: Safety-critical systems, formal methods and standards. Oxford University Technical Report PRG-TR-5-92, to appear in Software Engineering Journal.

[4] Dworatschek, Büllesbach, Koch u. a.: *Personal Computer und Datenschutz.* Datakontext-Verlag, Köln 1990.

[5] Winfried Gleißner, Rüdiger Grimm, Siegfried Herda, Hartmut Isselhorst: *Manipulation in Rechnern und Netzen.* Addison-Wesley, Bonn usw. 1989.

[6] H. Kopetz: Fehlertolerante Systeme. In: H. Maurer (Hrsg.): *Überblicke Informationsverarbeitung 1984,* BI-Wissenschaftsverlag, Mannheim usw. 1984, S. 75–94.

[7] Gunhild Lütge: Amoklauf der Maschinen. Die Zeit 2. April 1993, S. 23–24.

[8] Barton P. Miller, Lars Fredriksen, Bryan So: Fatale Fehlerträchtigkeit – Eine empirische Studie zur Zuverlässigkeit von Unix-Utilities. iX 3/1991, 104–116.

[9] Klaus Pommerening: *Datenschutz und Datensicherheit.* BI-Wissenschaftsverlag, Mannheim usw. 1991.

[10] Die Netnews-Gruppe 'comp.risks'. Archiv auf dem FTP-Server 'CRVAX. SRI.COM' im Verzeichnis 'RISKS:'.

[11] Die programmierte Katastrophe. Spiegel-Report über Fehleranfälligkeit von Computersystemen. Der Spiegel 42/1990, 80–93.

[12] Computer – Chaos machbar. Der Spiegel 25/1989, 185–186.

[13] Peter Paul Spies (Ed.): *Datenschutz und Datensicherung im Wandel der Informationstechnologien.* 1. GI-Fachtagung, München, Oktober 1985, Proceedings, Informatik-Fachberichte 113, Springer-Verlag, Berlin usw. 1985.

[14] Gerhard Weck: *Datensicherheit.* Leitfäden der angewandten Informatik, B. G. Teubner, Stuttgart 1984.

[15] Zentralstelle für Sicherheit in der Informationstechnik (Hrsg.): *IT-Sicherheitskriterien – Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT).* Bundesanzeiger, Köln 1989.

[16] Zentralstelle für Sicherheit in der Informationstechnik (Hrsg.): *IT-Evaluationshandbuch – Handbuch für die Prüfung der Sicherheit von Systemen der Informationstechnik (IT).* Bundesanzeiger, Köln 1990.