Datenschutz und Klinikvernetzung

Um Mißbrauch in Datennetzen vorzubeugen, müssen genaue Regeln aufgestellt werden – Folge 9 der RhÄ-Reihe „Medizin und Datenverarbeitung“

von Klaus Pommerening*

Informationsverarbeitende Systeme werden immer mehr miteinander vernetzt, lokal und global. Dadurch werden neue Möglichkeiten zur Effizienzsteigerung der medizinischen Versorgung geschaffen. Aber auch die Probleme dieser Technik werden immer deutlicher. Die Medizin mit ihren besonders hohen Datenschutzanforderungen, der ärztlichen Schweigepflicht und dem Anspruch, Schaden vom Patienten fernzuhalten, ist hier besonders betroffen.

Datenschutz und Datensicherheit? – Probleme der vernetzten Klinik

Das Problem der Datenzugriffsrechte ist eigentlich ganz einfach zu lösen: Jeder hat Zugriff auf genau die Daten, die er zur Erfüllung seiner Aufgabe braucht – das nennt man das Prinzip der minimalen Rechte. Umsetzen kann man es freilich nur, wenn man ein explizites, ausführliches Daten- und Rechtemodell, eine sogenannte Zugriffsmatrix hat und wenn die verwendeten Programme dieses Modell auch unterstützen. Die Zugriffsmatrix muß berücksichtigen, daß die Daten eines Patienten nicht über die unmittelbare Zweckbindung des Behandlungsvertrags hinweg weitergegeben werden dürfen, auch nicht an andere Fachabteilungen oder an die Krankenhausverwaltung. Die Verantwortung für die Daten liegt beim erhebenden Arzt bzw. der erhebenden Abteilung. Da die Daten eines Patienten zur rechten Zeit am rechten Ort verfügbar sein müssen, ist besonders für Notfallsituationen Vorsorge zu treffen, wo der Zugriff auf Daten unkompliziert sein muß.

Selbst wenn die Zugriffsrechte genau definiert sind, sieht es mit ihrer Absicherung in der Praxis gegenwärtig noch sehr traurig aus. Die gängige Software, gerade von führenden Herstellern, erlaubt unberechtigte Zugriffe auf vielfältige Weise. Zum Beispiel ist es schwierig, aus vorkonfigurierten Datenmasken unerwünschte Felder zu entfernen. Auch sehen die auf dem Markt dominierenden Schnittstellen für Datenbankzugriffe keine effektiven Möglichkeiten der Zugriffskontrolle vor. Dazu kommt, daß der allgemein noch übliche Paßwortschutz neben seiner umständlichen Handhabung auch viel zu wenig Sicherheit bietet, besonders wenn man Paßwörter mehrfach eingeben oder sich verschiedene Paßwörter merken muß.

Personal Computer, transportable Datenträger, lokale Netze, Modemanschlüsse und das Internet zählen zu den „offenen Systemen“. Immer mehr Tätigkeiten werden mit Standard-Software erledigt wie Datenbanksystemen, Tabellenkalkulation, Textverarbeitung. Diese Systeme sind auch im sicherheitstechnischen Sinne offen. Vor allem Systemverwalter, die ja eigentlich nicht zum Behandlungsteam gehören, können ohne Mühe alle Daten sehen. Gleiches gilt für Wartungstechniker und Netzpersonal.

Datenschutz und Datensicherheit? – Probleme der öffentlichen Netze

Im Zeitalter der zunehmenden Vernetzung des gesamten Gesundheitswesens, der integrierten Versorgung („shared care“) der Arbeitsteilung und der Gesundheitsreform kann ein Krankenhausinformationssystem nicht mehr als geschlossenes System betrachtet werden.

Die Patentlösung für diese Anforderungen scheint ein Internetanschluß zu sein. Die Fülle der inzwischen angebotenen medizinischen Informationen und die Leichtigkeit der Kommunikation machen den Verzicht auf den Anschluß bereits heute unwirtschaftlich. Gleichzeitig verbieten die Forderungen nach Sicherheit und Datenschutz diesen Anschluß aber geradezu, wenn man sich die inhärente Unsicherheit der gängigen Systeme und der Standard-Software vor Augen hält. Im Konkurrenzkampf um die Weltherrschaft im Internet gerät die Sicherheit vollends unter die Räder. So haben es die großen Software-Hersteller inzwischen geschafft, daß selbst die harmlose E-Mail zu einem unkontrollierbaren Sicherheitsproblem geworden ist. E-Mail kann heute als Anlagen alles mögliche vom Word-Dokument bis zu Ton-Dateien enthalten. Geht der Benutzer bei der Konfiguration nicht sehr sorgfältig vor, werden beim Lesen der Mail oft Programme auf seinem Rechner gestartet, deren Auswirkungen er nicht unter Kontrolle hat. Ganz schlimm ist die Entwicklung der letzten Zeit im Bereich der WorldWideWeb-Browser. Sicherheitslücken, insbesondere beim MS-Internet-Explorer, führen sogar dazu, daß externe Anbieter von Webseiten beliebige Programme auf dem Rechner des arglosen Internet-Surfers ausführen können.

Dagegen verblassen die „klassischen“ Probleme des Anschlusses an öffentliche Netze schon fast: einerseits die Gefahr, daß Klinikmitarbeiter Daten nach außen schmug-

*Prof. Dr. Klaus Pommerening lehrt an der Johannes-Gutenberg-Universität Mainz Medizin-Informatik und ist Leiter der GMDS-Arbeitsgruppe „Datenschutz in Gesundheitsinformationssystemen“

geln, etwa per E-Mail, und andererseits die leichte Abhörbarkeit der Netze. Gegen die erste dieser Gefahren helfen nur Verbote und die restriktive Handhabung der internen Zugriffsrechte. Und natürlich das Vertrauen darauf, daß jeder Arzt seine Schweigepflicht ernst nimmt. Die zweite Gefahr, die Abhörbarkeit von Datenübertragungen im Netz, ist in erster Linie durch technische Maßnahmen zu lösen, nämlich durch den Einsatz von kryptographischer Verschlüsselung. Dies ist zur Zeit leider noch mit etwas Aufwand verbunden.

Der Stand der Technik beim Internet-Anschluß

Eine saubere Lösung wäre ein Internet-Anschluß von wenigen und speziell dafür vorgesehenen Rechnern, die vom Kliniknetz isoliert sind. Das kann aber bei genauem Hinsehen nur eine vorübergehende Notlösung sein: Der flüssige Arbeitsablauf wird behindert, das Problem der Fernwartung bleibt ungelöst.

Der Kompromiß, der dem Stand der Technik entspricht, ist ein Internetanschluß über ein sogenanntes Firewall-System. Ein Firewall-System überwacht und filtert den Datenstrom. So wird das öffentliche Netz maximal genutzt und die Gefährdung minimiert: Aber cave! Es bleiben Gefahren, die nur durch sorgfältige System-Administration und Aufklärung der Mitarbeiter über zu vermeidende Techniken zu beherrschen sind. Die GMDS (Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie) Arbeitsgruppe „Datenschutz in Gesundheitsinformationssystemen“ hat Empfehlungen erarbeitet, von denen die wichtigsten hier aufgeführt seien:

- Außerhalb des durch die Firewall geschützten Bereiches dürfen keine personenbezogenen Daten des Krankenhauses gespeichert oder verarbeitet werden.
- Interaktive Dienste (z.B.: telnet, Zugriff auf News-, WWW- und externe Medline-Server) dürfen nur vermittelt werden, wenn die Kontaktaufnahme von der Klinik in die Außenwelt erfolgt, nicht umgekehrt.
- Die Einwahl von außen ins Kliniknetz, etwa zur Fernwartung, muß einer besonders strengen Überwachung unterliegen; eine sicherheitstechnisch akzeptable Lösung hierfür wird durch einen Modem-Server und die Vergabe von Einmal-Paßwörtern geschaffen.
- E-Mail soll in beiden Richtungen unbeschränkt möglich sein.

Die vollständige Version mit Begründung und Literaturhinweisen ist im Internet unter *http://www.uni-mainz.de/FB/Medizin/IMSD/AG-Datenschutz/Empfehlungen* zu finden.

Auf Benutzerseite ist unbedingt im E-Mail-Programm und im Web-Browser das automatische Anzeigen von eingebetteten Dokumenten (Word, PDF u. a.) zu sperren, denn gegen die hierin möglicherweise enthaltenen Schadprogramme und Viren kann die Firewall nicht zuverlässig schützen. Für den Betrieb von Firewall-Systemen sind betriebsintern klare Richtlinien und Zuständigkeitsregelungen zu definieren.

Der eigenständige Aufbau eines Firewall-Systems ist nur für Universitätskliniken mit entsprechend ausgebildetem Personal möglich und sinnvoll. Ansonsten wird auch eine große Klinik auf ein kommerziell angebotenes Firewall-System zurückgreifen, wobei Beschaffung, Konfiguration und Betrieb ein nicht zu unterschätzendes Maß an eigenem Know-How und Arbeitsaufwand erfordern. Für kleinere Häuser bleibt der Anschluß über einen Service-Anbieter, mit dem klare vertragliche Abmachungen über die Umsetzung der Sicherheitsanforderungen getroffen werden müssen.

Maßnahmen für die interne Sicherheit

Während wir für die Schaffung eines angemessenen technischen Sicherheitsniveaus weitgehend den System-Herstellern ausgeliefert sind, müssen die Betreiber eines informationstechnischen Systems für die organisatorische Sicherheit selbst sorgen. Das beginnt mit der Erstellung eines Sicherheitskonzepts. Dieses sollte enthalten:

- das Organisations- und Prozeßmodell des Betriebs,
- das Daten- und Datenflußmodell des Betriebs,
- Zugriffsprofile für Mitarbeitergruppen in Form einer Zugriffsmatrix,
- Grundsätze für die Anbindung ans Internet,
- Regelung der Zuständigkeiten im informationstechnischen Bereich,
- Management-, Prozeß- und Qualitätsbewertungskriterien.

Jede Institution des Gesundheitswesens braucht einen Datenschutzbeauftragten und einen IT (Informationstechnologie)-Sicherheitsverantwortlichen (Security Officer). Diese Aufgaben sind zu trennen, da der Datenschutzbeauftragte Kontrollinstanz ist und nicht gleichzeitig Ausführender sein kann. Beide Funktionsträger benötigen, abhängig von Größe und Struktur der Institution, für die Erfüllung ihrer Aufgaben ausreichend Zeit, Mittel und Unterstützung, insbesondere durch Schreibkräfte, sowie Durchsetzungsbefugnisse. Der Datenschutzbeauftragte hat die im zuständigen Datenschutzgesetz festgelegten Aufgaben. Er sollte Mediziner sein.

Der IT-Sicherheitsverantwortliche sollte Informatiker oder Medizin-Informatiker sein. Er erstellt das Datenschutz- und IT-Sicherheitskonzept der Institution, stimmt es mit dem Datenschutzbeauftragten ab, setzt es mit Hilfe des vorhandenen IT-Personals um und schreibt es fort. Unter anderem ist er verantwortlich für die physische Sicherheit der Rechner, Netze und Datenträger einschließlich Brandschutz und Schutz vor Naturgewalten, für die Anpassung der Systeme an das Sicherheitskonzept und für die Überwachung des lokalen Netzes auf unerwünschte Datenflüsse.

In großen Institutionen erfordern die Tätigkeiten des Datenschutzbeauftragten und des IT-Sicherheitsverantwortlichen je eine volle Stelle. In kleinen Institutionen stellt sich das Problem des Outsourcing in der Form des Heranziehens externer Sicherheitsberater. Hier sollte die Verantwortung auf jeden Fall im Hause bleiben. Beim Datenschutz wäre die Bestellung eines gemeinsamen Beauftragten für mehrere Häuser denkbar. Da die differenzierte Kenntnis der lokalen Verhältnisse wichtig ist, wird Outsourcing oft als wenig effektiv und zu teuer erachtet. Das ist das Dilemma der Sicherheit: Sie zu gewährleisten ist aufwendig, aber eigentlich nicht an Fremde übertragbar.

Die Abteilungsnetze sind nach Möglichkeit voreinander durch Router (Umleiter) und Netzbeschaffenheit abzusichern. Ist nur ein gemeinsames Klinikinformationssystem vorhanden, ist die Datenhoheit der Fachabteilungen in diesem zu berücksichtigen.

Die Sicherheitsmaßnahmen sollen die Aufmerksamkeit des Arztes nicht vom Patienten ablenken. Zwar ist Datenschutz ohne Mitwirkung der Beteiligten nicht zu verwirklichen, aber die Belastung des medizinischen Personals durch organisatorische und technische Verfahren sollte minimal bleiben. Der sachgerechte Umgang mit den Patientendaten darf durch Schutzmaßnahmen nicht beeinträchtigt werden. Die Verfügbarkeit der Daten, besonders in kritischen Situationen, ist im Interesse des Patienten zu gewährleisten.

Perspektiven

Die technische Entwicklung im Bereich der IT-Sicherheit ist zur Zeit in starker Bewegung. Der zunehmende Einsatz von Standard-Software führt zu immer größeren Sicherheitsproblemen und darüber hinaus zu einer wachsenden Abhängigkeit von den Herstellern. Allerdings wissen diese gerade im Bereich der Krankenhaus-Informationssysteme durchaus, was von ihnen verlangt wird und bemühen sich um Sicherheit. Was ihnen fehlt, sind zuverlässige Standards und ein Ende der politischen Debatte um eine mögliche gesetzliche Einschränkung der Zulässigkeit von Codierungsverfahren.

Aber es gibt auch eine Reihe von ermutigenden Entwicklungen. Auf dem konzeptionellen Sektor sind hier die SEISMED-Guidelines zu nennen, die eine gründliche Bestandsaufnahme dessen geben, was zur Erreichung von IT-Sicherheit im medizinischen Umfeld nötig ist. In Folgeprojekten soll die Praktikabilität dieser Leitlinien verbessert und die konkrete Umsetzung demonstriert werden.

HPCard konnte viele Funktionen übernehmen

Von besonderem Interesse und mit voraussichtlich sehr breiter Wirkung ist das HPC-Projekt („Health Professional Card"). Es zielt darauf ab, für Ärzte und andere Berufsgruppen im Gesundheitswesen eine Chipkarte als Berufsausweis einzuführen, der gleichzeitig die Grundfunktionen für die IT-Sicherheit bietet: sichere Authentifikation, elektronische Unterschrift und die dazu nötigen kryptographischen Verfahren und Schlüssel. Die praktische Erprobung hat im Magdeburger Tumorregister bereits begonnen. Ein Beschluß der Bundesärztekammer vom Frühjahr 1997 zielt auf die breite Einführung dieses elektronischen Berufsausweises bis 1999. IT-Systeme sollten heute schon für die Integration dieser Karten und der entsprechenden Sicherheitsfunktionen ausgelegt werden. Damit sollte der umständliche Umgang mit Paßwörtern der Vergangenheit angehören. Der Benutzer eines Krankenhausinformationssystems weist sich dann einmal pro Arbeitssitzung mit seiner Karte und seinem PIN-Code aus und hat dann alle ihm zustehenden Rechte.

Die Ausgabe der HPC und die Erzeugung der auf ihr enthaltenen, zum Teil geheimen, kryptographischen Schlüssel erfordert eine sichere Infrastruktur; man spricht von Trust-Center-Funktionen. Hier ist denkbar, daß die HPC als allgemeiner Berufsausweis von den Ärztekammern oder klinikintern ausgegeben wird.

Weiter auszubauen ist die kryptographische Infrastruktur. Denn grundsätzlich sollten Daten ausnahmslos verschlüsselt gespeichert und/oder übertragen werden. Die HPC bietet einen geeigneten Ansatz, dies ohne merkbare Belästigung der Benutzer zu erreichen, da sie die nötigen Schlüssel speichern kann. Auf diese Weise erledigen sich die Probleme der Dateneinsicht durch IT-Betriebspersonal und der Abhörbarkeit der Netze. Jeder Ansatz zur derzeit politisch diskutierten Schlüsselhinterlegung ist abzulehnen, da dies nicht mit der ärztlichen Schweigepflicht vereinbar ist.

Ein weiterer Ansatz zur Verbesserung des Datenschutzes ist die Verwendung von Pseudonymen statt Identitätsdaten, wo es immer möglich ist. Sie können zur Anonymisierung bei Forschungsprojekten, aber auch für die Krankenkassen-Abrechnung (!) verwendet werden. Auch im Krankenhausinformationssystem könnten Pseudonyme dazu dienen, die unmittelbar identifizierenden Daten vom Stammdatensatz zu trennen und so bei System-Wartungsarbeiten mit Echtdaten wenigstens ein Minimum an Datenschutz zu gewährleisten.

Die GMDS hat ein Grundsatzpapier mit Leitlinienfunktion zu Datenschutz und Datensicherheit in Informationssystemen des Gesundheitswesens erarbeitet und unter der Adresse *http://www.uni-mainz.de/FB/Medizin/IMSD/AGDatenschutz* mit weiteren Informationen und Empfehlungen bereitgestellt.

Anschrift des Verfassers:
Prof. Dr. Klaus Pommerening
Institut für Medizinische Statistik
und Dokumentation der
Johannes-Gutenberg-Universität
55101 Mainz