Datensicherheit

- Sicherheitskonzepte für das Krankenhausnetz und die externe Kommunikation -

Klaus Pommerening

Mit der zunehmenden Vernetzung von Krankenhäusern im Innern und nach außen stellen sich Datensicherheitsprobleme, die wegen der hohen Datenschutzanforderungen in der Medizin mit großer Sorgfalt behandelt werden müssen. Die GMDS-Arbeitsgruppe »Datenschutz in Gesundheitsinformationssystemen« hat dazu einige Empfehlungen erarbeitet, auf deren Grundlage die folgende zusammenfassende Darstellung entstanden ist. Die ausführliche Version der Empfehlungen ist in den Workshop-Unterlagen und über die WWW-Seite der Arbeitsgruppe zu finden:

```
http://www.uni-mainz.de/FB/Medizin/IMSD/AGDatenschutz
```

Dort findet man auch Literaturangaben und Verweise zu weiteren relevanten WWW-Quellen.

1. Grundsätze

1.1 Datenschutz und Datensicherheit

Die Datenschutzgesetzgebung verlangt, daß die Informationsverbeitung nur in einer Umgebung und auf Systemen erfolgt, die nach dem Stand der Technik abgesichert sind. Die gegenwärtige alltägliche Praxis ist hier leider in einem beklagenswerten Zustand. Es herrschen »offene Systeme« vor: Personal Computer, transportable Datenträger, lokale Netze, Modemanschlüsse, das Internet, und immer mehr Tätigkeiten werden mit Standard-Software erledigt. Diese Systeme sind auch im sicherheitstechnischen Sinne offen, und zwar bis zum letzten Bit. Die Verarbeitung und Speicherung von Daten in solchen offenen Systemen sind mit den Datenschutzvorschriften nicht zu vereinbaren, wenn nicht umfangreiche Sicherheitsvorkehrungen getroffen werden.

Die grundsätzlichen Anforderungen an die Datensicherheit sind

- Verfügbarkeit,
- Integrität,
- Verbindlichkeit,
- Vertraulichkeit.

Zur Verbindlichkeit gehören auch die Aspekte Beweissicherheit und Verantwortlichkeit. Zur Integrität gehört die Fälschungssicherheit und die Authentizität, auch von Identitäten (Personen und Maschinen).

1.2 Konzeption

Während wir uns für die Schaffung eines angemessenen technischen Sicherheitsniveaus weitgehend auf die System-Hersteller verlassen müssen, sind wir als Betreiber eines informationstechnischen Systems für die organisatorische Sicherheit selbst zuständig. 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 externe Vernetzung,
- Regelung der Zuständigkeiten im informationstechnischen Bereich,
- Management-, Prozeß- und Qualitätsbewertungskriterien.

Qualitätsmanagement und Systembewertung werden als Entwicklungsergebnis oft unterschätzt, sind jedoch von besonderer Bedeutung für den Erfolg eines Informationssystems.

Das Problem der Datenzugriffsrechte ist im Prinzip eigentlich ganz einfach zu lösen: Jeder hat Zugriff auf genau die Daten, die er zur Erfüllung seiner Aufgabe braucht - das ist 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 verwendete Software dieses Modell auch unterstützt. 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; mit dem Patienten kann er auch die Daten an einen Kollegen oder eine andere Abteilung überweisen, soweit sie dort für die Weiterbehandlung benötigt werden. Da die Daten eines Patienten zur rechten Zeit am rechten Ort verfügbar sein müssen, ist insbesondere für Notfallsituationen Vorsorge zu treffen, wo der Zugriff auf Daten unkompliziert sein muß. Ein Mißbrauch des Notfallzugriffs darf aber nicht folgenlos geschehen.

1.3 Organisation

Keine Sicherheitsmaßnahme kann etwas nützen, wenn die Verantwortung für ihre Einführung, Anwendung und Überwachung nicht klar geregelt ist. Das kann nur zum Teil von dem gesetzlich geforderten Datenschutzbeauftragten übernommen werden, der ja Jurist oder (in Einrichtungen des Gesundheitswesens) Mediziner sein sollte. Die SEISMED-Guidelines fordern außerdem einen IT-Sicherheitsbeauftragten, der Informatiker mit entsprechenden Fachkenntnissen sein sollte. Er hat die Federführung bei der Erstellung des Sicherheitskonzepts, sorgt für die physische Sicherheit von Rechnern, Netzen und Datenträgern, kontrolliert die Sicherheit von Datenarchiven, sorgt dafür, daß die Konfiguration der Systeme dem Sicherheitskonzept entspricht und nicht irgendwelche Systemvoreinstellungen Sicherheitslücken aufreißen, überwacht das lokale Netz, insbesondere auf ungenehmigte Modems, verwaltet die zukünftigen elektronischen Ausweiskarten, wertet sicherheitsrelevante Systemaufzeichnungen aus, kontrolliert die Implementation von Software, schult IT-Personal und Benutzer, motiviert sie zum sorgfältigen Umgang mit Gefahrenquellen und berät den Datenschutzbeauftragten und die Personalvertretung in technischen Fragen und bei der Formulierung von Verpflichtungserklärungen. Auch einzelne Fachabteilungen im Krankenhaus müssen für diese Aufgaben einen angemessenen Anteil an Personalkapazität einplanen.

2. Sicherheitsempfehlungen zu Abteilungsnetzen im Krankenhaus

Client-Server-Systeme werden meist auf der Basis von Unix- oder Windows-NT-Servern betrieben. Dabei treten, meist durch mangelnde Fachkenntnis des IT-Personals, aber auch aufgrund von Sicherheitslücken, vor allem in Windows NT, Sicherheitsprobleme auf, die wirksamen Datenschutz verhindern. Die Konfiguration eines einigermaßen sicheren lokalen Netzes ist komplex und aufwendig. Dieser Aufwand ist aber aufgrund der Datenschutzvorschriften unumgänglich, sobald Patientendaten auf dem Rechner gespeichert oder verarbeitet werden; er sollte auch in allen anderen Fällen im eigenen Interesse nicht gescheut werden und erfordert in jedem Fall eine Vollzeitstelle für einen Systemverwalter. In diesem Abschnitt kann das Thema bei weitem nicht erschöpfend behandelt werden; für weitere Informationen sind die in den Workshop-Unterlagen und auf den WWW-Seiten aufgeführten Verweise geeignet.

Die Abteilungsnetze sind nach Möglichkeit voreinander durch Router und Netztopologie abzusichern. Ist, wie in kleineren Häusern oft anzutreffen, nur ein gemeinsames Kliniksinformationssystem vorhanden, ist die Datenhoheit der Fachabteilungen in diesem zu berücksichtigen.

2.1 Grundsätzliches zur Sicherheit von Unix und NT

Windows NT wird oft als sicheres Betriebssystem angepriesen. In der Tat bietet NT einige Sicherheitsmechanismen, die für IT-Betreiber, die MS-DOS, Windows 3 oder Windows 95 gewöhnt sind, sehr eindrucksvoll wirken. Dieser Eindruck ist aber irreführend, zumal die Systemvoreinstellungen nur wenige der möglichen Sicherheitsschranken in Kraft setzen. Die in der Werbung angepriesene und in manchen Fachbüchern unkritisch angenommene C2-Sicherheit gilt nur nach ganz besonderen Maßnahmen, z. B. der völligen Trennung

vom Netz, die das System in einen praktisch unbrauchbaren Zustand versetzen. Ebenso wird die Sicherheit eines NT-Systems durch Installation und Betrieb von Anwendungssoftware in der Regel unterlaufen; manche Anwendungssoftware funktioniert sogar nur mit unsicheren System-Einstellungen. Werden im Netz auch Windows-95-Rechner betrieben, sinkt das Sicherheitsniveau weiter. Auch die durch die Benutzungsoberfläche, besonders ab NT-Version 4.0, suggerierte Leichtigkeit der Konfiguration ist irreführend und gefährlich, da sie Nachlässigkeit provoziert.

Die NT-Sicherheitsmechanismen können bei sorgfältiger Einstellung ungefähr das Niveau gewöhnlicher Unix-Systeme erreichen; einiges ist etwas besser, einiges etwas schlechter geregelt. Auf der praktischen Seite sind aber erhebliche Defizite bei der Zuverlässigkeit der Implementation zu bemängeln. Zahlreiche konzeptionelle Sicherheitslücken und Implementationsfehler stellen NT auf eine Stufe mit älteren Unix-Systemen. Als Server sind daher aktuelle Unix-Systeme, insbesondere Linux, zu empfehlen. Die mit den Workshop-Unterlagen verteilten konkreten Ratschläge gelten für den Fall, daß trotzdem ein Netz auf NT-Basis betrieben werden muß.

Um die Sicherheitsmechanismen von Unix oder NT wirkungsvoll einzusetzen, ist eine ausführliche Planung, insbesondere der Zugriffsrechte, und eine sehr sorgfältige Umsetzung nötig. Das Prinzip der minimalen Rechte sollte bei der Zugriffsregelung strikt beachtet werden. Im Netz sollte genau festgelegt werden, welcher Rechner in welche anderen welches Ausmaß an Vertrauen setzt und welche Ressourcen an ihn freigegeben werden. Ebenso sollten die Benutzer-Zugriffsrechte auf Ressourcen und Verzeichnisse in einer Rechte-Matrix spezifiziert werden.

Es sollte stets eine ausgedruckte Version der System-Konfiguration einschließlich Vernetzungsplan und eine exakte Beschreibung der »Sicherheitspolitik« zur Hand sein. Die Konfiguration sollte sorgfältig dokumentiert sein, insbesondere die Sicherheitsmaßnahmen.

Um über aktuelle Sicherheitsfragen stets auf dem laufenden zu sein, ist es notwendig, daß der Systemverwalter mindestens eine einschlägige Usenet-Newsgruppe oder Mail-Liste verfolgt.

2.2 Sicherheitsratschläge für den Systemadministrator

Systemverwalter sollten eine Benutzer-Kennung mit Administrator-Rechten nur für wirkliche Verwaltungsaufgaben nutzen. Für Arbeiten, die nicht die vollen Privilegien benötigen, sind gewöhnliche Benutzer-Kennungen zu verwenden. Insbesondere sollte unter Administrator-Rechten nicht mit Anwendungen gearbeitet werden, die für das Einschleusen von Schadprogrammen anfällig sind, wie die MS-Office-Anwendungen, E-Mail oder WWW-Browser.

An Servern sollte, außer für Administrator-Aufgaben, nicht lokal gearbeitet werden. Bei der Unterbrechung von Systemadministrator-Arbeiten sollte ein Logout ausgeführt oder (bei NT) im Task-Manager die Arbeitsstation gesperrt werden.

Um das Aussperren des Systemverwalters und als Folge möglicherweise eine längerdauernde Nichtverfügbarkeit des Rechners zu verhindern, ist für diesen eine Paßwortsperre nach mehreren Fehlversuchen nicht sinnvoll. Daher sollte man dessen Logon nur lokal zulassen. Um auch in Notfällen Administrator-Aufgaben wahrnehmen zu können, sollte das Administrator-Paßwort in einem versiegelten Umschlag an sicherer Stelle, z. B. in einem Safe, hinterlegt werden. Gleiches gilt für ein eventuelles Hardware-Paßwort und für Schlüssel zu Zugangstüren oder Rechnergehäuse.

Eine Anmeldung über das Netz oder gar über eine unverschlüsselte Fernverbindung (mit RAS-Berechtigung) ist unter Sicherheitsgesichtspunkten besonders kritisch zu werten. Daher ist der Fernzugriff für den Systemverwalter zu sperren. Eine alternative Maßnahme ist die Einrichtung einer anderen Kennung mit Administrator-Rechten, für die der Zugang über das Netz möglich ist, allerdings die Paßwortsperre bei Fehlversuchen funktioniert.

Mitarbeiter sollten auf ihren Arbeitsplatzrechnern keine, auch nicht die lokale, Administrator-Berechtigung

erhalten; Ausnahmen sind nur bei besonderen Systemkenntnissen möglich.

3. Sicherheitsempfehlungen zu Modem-Verbindungen im Krankenhaus

Aus verschiedenen Gründen kann für Rechner in einem Krankenhaus ein Modem-Anschluß wünschenswert sein:

- Zugriff auf externe Informationen im Internet,
- Systemverwaltungsarbeiten in Heimarbeit,
- Anwendungsbearbeitung in Heimarbeit,
- Fernwartung durch Firmen,
- Telemedizinische Anwendungen.

Dabei entstehen erhebliche Sicherheitsrisiken, sowohl für den Schutz der Patientendaten und anderer personenbezogener Daten als auch für die Integrität der angeschlossenen Rechner und des gesamten Krankenhaus-Informationssystems, die besonders sorgfältige Planung, Konfiguration und Dokumentation erfordern.

3.1 Grundsätze zum Modem-Anschluß

»Remote Access Server« (RAS) und Modems besitzen umfangreiche und sehr komplexe Konfigurationsmöglichkeiten, wobei die Voreinstellungen oft unsicher sind. Die zuverlässige Konfiguration erfordert erhebliche Systemkenntnisse und Sorgfalt. Da Sicherheitsprobleme nur in einer möglichst einfachen Konstellation beherrschbar bleiben, ist ein zentraler Modem- und Access-Server einzurichten, der unter der Verantwortung einer geeigneten Stelle im Krankenhaus (Rechenzentrum, zentrale Service-Abteilung) betrieben wird. Diese Stelle ist so auszustatten, daß sie die nötige Kompetenz erwerben kann.

Weitere Modem-Verbindungen sind in der Regel zu verhindern, weil sie die Sicherheit des gesamten Klinikinformationssystems unkontrolliert untergraben können. Ausnahmen von dieser Regel können gestattet werden

- für Rechner, die in der Klinik nicht weiter vernetzt sind und auf denen keine personenbezogenen Daten gespeichert sind - etwa zur Informationssuche im Internet, wenn keine andere Möglichkeit besteht,
- in begründeten Ausnahmefällen, sofern die unten aufgeführten Maßnahmen getroffen sind und die Möglichkeiten eines sicheren Firewall-Tunnels nicht genützt werden können - etwa um einen 24-Stunden-Notdienst an wichtigen Systemen zu gewährleisten oder wenn eine Fernwartungsverbindung über den zentralen Modemserver nicht möglich ist.

Konkrete technische Anforderungen an einen Modem-Anschluß sind in den Workshop-Unterlagen enthalten. Hingewiesen werden soll auch auf den Abschnitt über Modems im IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

3.2 Anwendungsfälle

3.2.1 *Systemverwaltung*

Ein Fernzugriff ist nur bei gründlicher Sachkenntnis zuzulassen. In diesem Fall ist der Zugriff über einen sicheren Firewall-Tunnel oder, soweit das nicht möglich ist, über ein Einzelmodem mit direkter Verbindungsschaltung vorzuziehen. Für die Verwendung eines privaten Rechners gilt das in 3.2.2 gesagte.

3.2.2 *Anwendungsbearbeitung*

Die Notwendigkeit zum Fernzugriff ist besonders gründlich zu prüfen. Der Zugang über einen sicheren Firewall-Tunnel oder den Modemserver mit RAS sollte dann obligatorisch sein. Ein privater PC darf für diesen Anwendungsfall nicht verwendet werden; wegen der Beschlagnahmeproblematik muß der Rechner dem Krankenhaus gehören und inventarisiert sein. Er unterliegt dann auch der Kontrolle durch den

Datenschutzbeauftragten des Krankenhauses.

3.2.3 *Fernwartung*

Fernwartung ist rechtlich unter dem Gesichtspunkt der Auftragsdatenverarbeitung zu sehen. Auftragsdatenverarbeitung und Fernwartung sollten in ihren Modalitäten in einem rechtsverbindlichen Vertrag festgelegt werden, insbesondere, wenn personenbezogene Daten verarbeitet werden. Dieser Vertrag sollte enthalten:

- Festlegung der Beteiligten, die persönlich zu benennen und zu verpflichten sind,
- Festlegung des Umfanges der Datenverarbeitung,
- Festlegung der Verantwortlichen und ihrer Stellvertreter,
- Organisation der Datenübermittlung.

Die Sicherheitsanforderungen sind in der Regel über ein Einzelmodem mit direkter Verbindungsschaltung am besten erfüllbar. Bei der Konfiguration kann, nach entsprechender vertraglicher Gestaltung, auf die Sachkenntnis der externen Firma zugegriffen werden. Die Anmietung eines Raumes bei der Firma durch das Krankenhaus zum Zweck der Fernwartung ist zu empfehlen. Die Fernwartung ist abzustufen nach

- Hardware,
- Betriebssystem,
- Anwendungssoftware;

nur die jeweils unbedingt nötigen Zugriffe sind zu gewähren. Es ist in jedem Fall sicherzustellen, daß kein Zugriff auf Patientendaten erfolgen kann. Die Fernwartungsaktivitäten sind lokal durch einen Systemverantwortlichen mitzuverfolgen, der gegebenenfalls die Verbindung sofort unterbrechen kann; sie sind außerdem automatisch zu protokollieren. Nach Möglichkeit ist ein Testsystem bereitzustellen; nach Abschluß der Wartung werden dann die ˜nderungen vom lokalen IT-Personal in das Produktionssystem übernommen. Auf diese Weise wird auch die Stabilität des Produktionssystems besser gewährleistet.

Fernwartungsverbindungen sollen nur vom Krankenhaus her aufgebaut werden dürfen; ein beliebiges Einwählen durch die beauftragte Firma ist abzulehnen. Die Modemverbindung sollte außer im unmittelbaren Anwendungsfall physisch unterbrochen sein.

Zum Thema »Fernwartung« gibt es eine Reihe von Stellungnahmen der Landesdatenschutzbeauftragten, insbesondere Leitlinien des Landesbeauftragten für den Datenschutz Bremen, die von der Konferenz der Datenschutzbeauftragten zustimmend zur Kenntnis genommen wurden und von der Arbeitsgruppe unterstützt werden.

3.2.4 *Telemedizinische Anwendungen*

Hier ist die Verbindung grundsätzlich über den Modemserver und RAS aufzubauen. Eine besonders gründliche IP-Nummern-Kontrolle ist vorzusehen.

4. Sicherheitsempfehlungen zum Internet-Anschluß von Krankenhäusern

Die Menge der im Internet angebotenen nützlichen medizinischen Informationen wächst rasch; mittelfristig soll das gesamte Gesundheitswesen von der Vernetzung profitieren. Daher ist der Internet-Anschluß von Krankenhäusern in den Bereich des Wünschenswerten gerückt.

Diese Entwicklung kollidiert aber mit den Datenschutz- und -sicherheitsanforderungen eines Krankenhauses. Bei unvorsichtigem Direktanschluß sind alle Daten auf lokalen Rechnern und Netzen gefährdet; sie können ausgespäht oder von unbefugten Internet-Teilnehmern unbemerkt verfälscht werden. Diese berechtigten Sicherheitsbedenken haben viele Verantwortliche bisher von einem Anschluß absehen lassen.

Die vom Internet ausgehenden Gefahren können wesentlich reduziert werden, wenn der Anschluß über ein sogenanntes Firewall-System vorgenommen wird. Dieses besteht aus einer Kombination von Routern mit einem Gateway-Rechner. Bei sorgfältiger Konfiguration kann dieses Vorgehen als ausreichende Sicherheitsvorkehrung gegen Hacker-Angriffe aus dem Internet angesehen werden. Datenschutz und Sicherheit im lokalen Netz werden dadurch aber in keiner Weise verbessert; hierfür sind gesonderte Maßnahmen erforderlich, die in Abschnitt 2 beschrieben wurden.

4.1 Grundsätze zur sicheren Internet-Anbindung

Die Anbindung an das Internet hat das Ziel: Möglichst komfortable Nutzung der Internet-Dienste bei möglichst großer Sicherheit vor unbefugten Zugriffen von außen. Es ist sorgfältig zu prüfen, welche Internet-Dienste wirklich benötigt werden. Konkrete Empfehlungen sind:

- Außerhalb des durch den Firewall geschützten Bereiches dürfen keine personenbezogenen Daten gespeichert oder verarbeitet werden.
- Interaktive Dienste (telnet, ftp, Zugriff auf News-, WWW- und externe Medline-Server) sollen nur vermittelt werden, wenn die Kontaktaufnahme von der Klinik in die Außenwelt erfolgt, nicht umgekehrt. Ausnahmen können mit den in Abschnitt 3 behandelten Maßnahmen zugelassen werden.
- E-Mail soll in beiden Richtungen unbeschränkt möglich sein.
- Erlaubt ist nur das TCP/IP-Protokoll; andere Protokolle (z. B. Novell-IPX, NetBEUI) werden gesperrt.
- Dienste, die nur im lokalen Netz benötigt werden und gefährliche Sicherheitslücken haben, werden gesperrt. (Beispiele: tftp, finger, NFS, NIS, X).
- Ebenso werden Java, JavaScript und ActiveX gesperrt. Der MS-Internet-Explorer ist wegen seiner Sicherheitslücken zu vermeiden.
- Eigene Informationsangebote der Klinik (z. B. WWW- oder FTP-Server) sind vor dem Firewall anzusiedeln. Hier sind selbstverständlich die Datenschutzvorschriften zu beachten; insbesondere dürfen keine personenbezogenen Daten bereitgestellt werden.
- Ist für die Klinik ein einziger Mail-Server ausreichend, kann dieser sowohl vor als auch hinter dem Firewall-System angesiedelt sein.
- Für den Betrieb von Firewall-Systemen sind betriebsintern klare Richtlinien und Zuständigkeitsregelungen zu definieren. Diese sollen auch Vorschriften über die Protokollierung, die Behandlung von sicherheitsrelevanten Ereignissen und Sanktionen bei Sicherheitsverstößen enthalten.

Die dem Stand der Technik entsprechende Konfiguration ist:

Innennetz <---> Router <---> Gateway <---> Router <---> Außennetz

Die dabei auftretende Redundanz in den Sicherheitsmaßnahmen ist erwünscht.

Durch dieses Konzept wird der völlig freie Internet-Zugang zugunsten der Sicherheit etwas behindert; die Unannehmlichkeiten halten sich aber in Grenzen und müssen im Hinblick auf Datenschutz- und Sicherheitsanforderungen einer Klinik in Kauf genommen werden.

Die Begründung dieser Empfehlungen ist in den Workshop-Unterlagen zu finden.

4.2 Realisierung

An der Universitätsklinik Mainz steht eine Referenz-Installation zur Verfügung. Bei dieser wird der Gateway auf einem Intel-Rechner unter Linux mit dem frei verfügbaren TIS-fwtk (Firewall Toolkit) realisiert. Dieses Vorgehen ist möglich, wenn genügend gute Unix-Kenntnisse vorhanden sind; andernfalls ist der Einsatz eines kommerziellen Firewall-Systems vorzuziehen. Die Hauptarbeit steckt aber in der Konfiguration, so daß die Arbeitseinsparung durch ein kommerzielles System eher gering ist; die Lieferfirma sollte daher auch Beratung, Schulung und Konfigurationshilfen anbieten.

An größeren Kliniken mit geschultem informationstechnischen Personal sind Abweichungen von den

Empfehlungen in 4.1 denkbar, wenn sie auf einer definierten Sicherheitspolitik beruhen und in ihren Auswirkungen beherrscht werden. So ist es bei geeigneten baulichen Voraussetzungen durchaus möglich, für einen Teil des Netzes, auf dem dann aber keine personenbezogenen Daten gespeichert oder verarbeitet werden dürfen, einen weniger restriktiven Internet-Anschluß zu schalten; die Kommunikation zwischen diesem Bereich und dem stärker geschützten muß mit besonderer Sorgfalt geregelt werden.