Erfahrungen bei der Erstellung und Umsetzung von Sicherheitskonzepten in Medizinischen Forschungsnetzen

Speer R[1], Dolak W[2]
[1]*Koordinierungszentrum für Klinische Studien, Universität Leipzig*
[2]*Institut für Medizinische Informatik, Statistik und Epidemiologie, Universität Leipzig, Deutschland*
ronald.speer@kksl.uni-leipzig.de

Einleitung und Fragestellung Die für medizinische Forschungsverbünde typische vernetzte rechnergestützte Verarbeitung und Speicherung personenbezogener Daten erfordert eine Vielzahl von Vorkehrungen, um die hohen Anforderungen an den Datenschutz und die Datensicherheit zu erfüllen. Um die Qualität der getroffenen Maßnahmen für die Auftraggeber sowie die Partner und Auftragnehmer (z.B. Patienten, Ärzte, Industrie) transparent und nachvollziehbar zu machen, ist das Erstellen geeigneter Datenschutz- und Datensicherheitskonzepte mit entsprechender Prüfung notwendig.
Vorschriften und Maßnahmen zur Datensicherheit in der klinischen Forschung und Versorgung tragen dazu bei, dass das Vertrauensverhältnis zwischen Patient und Arzt und das Persönlichkeitsrecht des Patienten bei der Datenverarbeitung gewahrt bleiben. Patientendaten sind nach dem Stand der Technik zu schützen, wobei aber das Prinzip der Verhältnismäßigkeit zu beachten ist. Insbesondere für medizinische Daten ist wegen ihrer Sensitivität ein entsprechend hoher Aufwand zur Realisierung der Sicherheit geboten. Durch technische und organisatorische Maßnahmen muss gewährleistet sein, dass nur die berechtigten Personen Zugriff auf die Daten erhalten.
Die Risiken, die durch die Informationstechnik in der klinischen Forschung und Versorgung drohen, sind vor allem:

- die Gefährdung der Patienten durch fehlerhafte Prozeduren oder unrichtige sowie unvollständige Daten,
- die Nichtnachvollziehbarkeit der Verantwortung von Maßnahmen,
- die Bedrohung der Vertraulichkeit, insbesondere die Verletzung der Schweigepflicht und des Datenschutzes,
- die Nichtverfügbarkeit von Daten oder des Informationssystems.

Unter dem Gesichtspunkt der in der klinischen Forschung und Versorgung erforderlichen Sicherheit muss der Realisierung von informationstechnischen Lösungen im Rahmen der medizinischen Forschungsverbünde eine klare Konzeption vorausgehen. In dieser Konzeption müssen die möglichen Risiken identifiziert und die notwendigen Maßnahmen benannt werden.

Material und Methoden
Am Institut für Medizinische Informatik, Statistik und Epidemiologie (IMISE) der Universität Leipzig werden in einem IT-Verbund mit dem Koordinierungszentrum für klinische Studien Leipzig (KKSL) Dienste und Datenbanken für verschiedene medizinische Forschungsverbünde (z.B. Kompetenznetz (KN) Lymphome, KN Sepsis, KN Herzinsuffizienz) bereitgestellt. Somit war die Erstellung eines Sicherheitskonzeptes für die Einhaltung der Forderungen des Datenschutzes und der Datensicherheit und als Grundlage der Vereinbarungen zwischen den Partnern eine wesentliche Forderung. Voraussetzung war die Initiierung eines IT-Sicherheitsmanagementprozesses, dessen wesentliche Aufgabe die Erstellung und Umsetzung eines Sicherheitskonzeptes war, und der dauerhafte Erhalt des angestrebten Sicherheitsniveaus auf Basis des erarbeiteten Sicherheitskonzeptes.
Die Einführung von IT-Lösungen orientiert sich in der Regel an den Zielen und Prozessen der betroffenen Institution. Somit ist die klare und vollständige Beschreibung der Unternehmensrichtlinien eine der ersten Maßnahmen. Weiterhin muss das Augenmerk auf die komplexe Prozessanalyse einschließlich der Integrationsmechanismen gerichtet sein. In dem nächsten Schritt sind eine generelle Risikoanalyse des Systems und seiner Umgebung sowie die Definition von Bedrohungen und Gegenmaßnahmen durchzuführen [1]. Die eindeutige Zuweisung und Beschreibung von Verantwortlichkeiten innerhalb der Institution und bei den Partnern ist eine entscheidende Voraussetzung für die Entwicklung und Implementierung sicherer IT-Lösungen.
Ausgangslage für ein funktionierendes Risikomanagement in der Informationstechnologie ist zunächst eine Risikoanalyse unter Einbeziehung aller von der IT unterstützten Prozesse. Aus dieser globalen Risikoanalyse ließen sich dann die für den Ist-Zustand notwendige Maßnahmen ableiten. Die Risikoanalyse ist die Grundlage für eine IT-Sicherheitsorganisation, die wiederum für die Erfassung und Beurteilung der aktuellen Risiken verantwortlich ist und darauf reagieren muss.
Für die Konzeption einer derartigen IT-Sicherheitsorganisation gibt es verschiedene Ansätze [6]:

- IT-Grundschutzhandbuch
  Durch das Bundesamt für Sicherheit in der Informationstechnologie (BSI) wurde ein sehr umfassendes Handbuch für die Erstellung von Sicherheitskonzepten entwickelt. Dieses IT-Grundschutzhandbuch [4] bildete mit seinen sehr detaillierten Handlungsanweisungen eine ideale Grundlage für das Rahmenkonzept. Es bietet aufgrund seiner offenen Definition bei der Modellierung des IT-Verbundes große Freiheiten.
- Alternative Ansätze
  Alternativ zu dem Technikorientierten Ansatzes des BSI-Grundschutzhandbuches existieren alternative Ansätze. Diese gehen aber im Gegensatz zu dem praxisorientierten Ansatzes des BSI-Grundschutzhandbuches, welches für die Umsetzung einer Standardsicherheit ganz konkrete Maßnahmen empfiehlt, nicht ganz so in die Tiefe. Neben dem US-amerikanischen COBIT [3] ist hier vor allem der Britische Standard BS7799 [2] zu nennen, dessen erster Teil seit dem Jahr 2000 als internationale Norm von der ISO/IEC angenommen wurde. Dadurch stellt BS7799 eine international anerkannte Norm (ISO/IEC 17799) für die Errichtung eines Informationssicherheits-Managementsystems (ISMS) dar.
  Die Detaillierungstiefe und die Strukturierung von BS7799 zielen vor allem auf die Aufrechterhaltung eines angemessenen Sicherheitsstandards ab und betont noch mehr die Verankerung des Sicherheitsmanagements in die Organisation der Institution. Somit ist für die Etablierung und den Betrieb von IT-Sicherheitsmaßnahmen und den Aufbau eines IT-Sicherheitsprozesses im Wesentlichen das BSI-Grundschutzhandbuch mit der Ergänzung durch ISO/IEC 17799 sinnvoll[5].

Ergebnisse
Für die Erstellung eines Sicherheitskonzeptes für den IT-Verbund IMISE/KKSL wurde der methodische Ansatz des Grundschutzhandbuches des BSI ausgewählt. Das modular aufgebaute IT-Grundschutzhandbuch spiegelt den Stand der Technik für die Erstellung eines Sicherheitskonzeptes für Unternehmen und Behörden mit mittlerem Schutzbedarf wider, ermöglicht darüber hinaus aber auch die Erweiterung um Sicherheitsmaßnahmen für die Verarbeitung, Speicherung und Übertragung von Daten mit hohem Schutzbedarf (z.B. personenbezogene Daten). Die Entscheidung für das Grundschutzhandbuches öffnet den Weg zu einer späteren Zertifizierung des IT-Sicherheitsniveaus durch das BSI. Im nächsten Schritt erfolgte eine umfassende Strukturanalyse und Schutzbedarfsfeststellung aller IT-Komponenten (Infrastruktur, Netzwerk, IT-Systeme, Anwendungen), die Erkennung der Gefährdungen, die Umsetzung der Sicherheits-Maßnahmen, die Überwachung des Umsetzungsgrades, die Dokumentation des IT-Sicherheitsstatus und die Zuordnung der Verantwortlichkeiten. Zur Qualitätssicherung und Unterstützung dieses Dokumentationsprozesses wurde ein vom BSI empfohlenes Softwarewerkzeug (GSTOOL) eingesetzt, das die gemeinsame Arbeit des Sicherheitsmanagement-Teams an allen Modulen ermöglicht.
Für die Sicherung des hohen Schutzbedarfes wurden zusätzliche Regelungen für besonders sensible Komponenten (Firewall, Datensicherheitskonzept, Konfigurationskonzept u.a.) durch gesonderte Einzelkonzepte berücksichtigt. Bei diesen Regelungen handelt es sich unter anderem um Konzepte für die Datensicherung, den Virenschutz und den Datenaustausch. Weiterhin wurden Regelungen für Notfälle und die Wartung der Systeme erarbeitet.
Das erstellte Sicherheitskonzept wurde im Rahmen von internen und externen Audits überprüft und ständig weiterentwickelt. Ebenfalls erfolgte eine Zertifizierung des Konzeptes durch das BSI im Rahmen einer Selbsterklärung.

Diskussion
Ein wesentliches Problem beim Einsatz des IT-Grundschutzhandbuches besteht darin, das es nur einen niedriger bzw. mittlerer Schutzbedarf abgedeckt. Bei den Forschungsverbünden entsteht aber aufgrund der verarbeiteten personenbezogenen Daten von Patienten ein hoher Schutzbedarf. Somit ist eine Erweiterung der Maßnahmen des IT-Grundschutzhandbuches um entsprechende Konzepte notwendig.

Das BSI-Grundschutzhandbuch hat sich dennoch mit seinen detaillierten Handlungsanweisungen als gute Grundlage für die Erstellung eines Wohlstrukturierten Sicherheitskonzeptes erwiesen. Aufgrund der modularen Struktur und den zur Verfügung stehenden Dokumenten und Werkzeugen ist es möglich auf der Basis des IT-Grundschutzhandbuches ein Sicherheitskonzept für einen medizinischen Forschungsverbund zu entwickeln. Insbesondere kann durch die detaillierten Handlungsanweisungen wird der Anwender bei der Umsetzung unterstützt.
Damit der Forschungsverbund Transparenz hinsichtlich der Sicherheitseigenschaften seiner IT-Lösungen schaffen kann ist eine Prüfung und Bewertung der Sicherheitsmaßnahmen nach einheitlichen Kriterien notwendig. Auf der Grundlage des IT-Grundschutzhandbuches vergibt das Bundesamt für Informationssicherheit (BSI) ein IT-Grundschutz-Zertifikat. Dieses Zertifikat ist der Nachweis über das erreichte Sicherheitsniveau. Somit kann ein Forschungsverbund mit vergleichsweise geringem Aufwand einen transparenten Nachweis über das im Rahmen ihres Sicherheitskonzeptes erreichte Sicherheitsniveau führen.
Durch entsprechende Auditingkonzepte bietet das IT-Grundschutzhandbuch ebenfalls die Möglichkeit der Selbstkontrolle und somit eine überprüfbare Qualität des Sicherheitskonzeptes.

Literatur

[1] Blobel B, Pommerening K. Datenschutz und Datensicherheit in Informationssystemen des Gesundheitswesens. Führen & Wirtschaften im Krankenhaus 2/1997: 133-138.
[2] BS7799, British Standards Institution, http://www.bsi-global.com
[3] COBIT, Control Objectives for Information and related Technology, http://www.isaca.org/cobitonline.
[4] Grundschutzhandbuch des BSI. Bundesamt für Sicherheit in der Informationstechnik. Stand Dezember 2005, http://www.bsi.de/gshb/deutsch/menue.htm. Berlin 2006
[5] Hoff S, Mohn P. IT-Sicherheitsüberprüfungen Mehr als ein notwendiges Übel!. Der Netwerk Insider. Mai 2003
[6] http://www.initiatived21.de/arbeitsgruppen/5sicherheit/leitfaden.pdf
[7] Speer R, Dolak W, Heller B, Meineke F, Ramsch J. Sicherheitskonzepte in medizinischen Forschungsverbünden. Telemed 2003. 8.Fortbildungsveranstaltung und Arbeitstagung. Tagungsband. Berlin, 2003: 101-103.