Empfehlungen zur IT-Sicherheit von Praxis-Systemen

Matthias Herbst, Stephen D. Wolthusen

Im Interesse gesteigerter Effizienz der medizinischen Versorgung und der Verwaltung der erbrachten und zu erbringenden Leistungen ist die Verwendung elektronischer Praxis-Systeme kaum zu vermeiden. Dadurch werden Datenbestände, für die nur unzureichende oder keine analogen Rückfallmechanismen existieren, insbesondere auch im Bereich einzelner Arztpraxen (in geringerem Umfang auch in Kliniken) verwaltet, deren Sicherheit gewährleistet werden muss.

Insbesondere sind dabei die folgenden Aspekte von Interesse:

- Gewährleistung von Vertraulichkeit von Patientendaten durch technische Mittel. Hier fordert der Gesetzgeber besondere Sorgfaltspflichten, denen insbesondere bei der Verwaltung dieser Daten in vernetzten IT-Systemen neue Herausforderungen gegenüberstehen. Hierzu ist eine wirksame Zugangs- und Zugriffskontrolle zum IT-System erforderlich, die sich insbesondere auch auf vernetzte Systeme oder bewegliche Datenträger erstrecken muss.
- Schutz der Integrität sowohl von Patientendaten als auch von Abrechnungsdaten. Dies betrifft mehrere potentielle Problembereiche, so etwa die Übermittlung von Abrechnungsdaten an kassenärztliche Vereinigungen, insbesondere aber die Datenhaltung innerhalb der ärztlichen Praxis. Die sensiblen Daten sind im Fall von Abrechnungsdaten über mehrere Monate in der unmittelbaren Kontrolle des IT-Systems, bei Patientendaten wie etwa Arztbriefen oder aber auch diagnostischen Hilfsmitteln wie digitalen Photographien müssen Aufbewahrungsfristen eingehalten werden. Bedrohungen der Integrität bestehen so etwa bei Manipulation (zwar potentiell auch durch Mitarbeiter, insbesondere jedoch aber durch unbeaufsichtigte Personen, z.B. zur Erlangung von BtM-Rezepten), insbesondere aber durch Fehler im IT-System (z.B. schrittweise Korrumpierung von Datenbank-Datensätzen) oder mittelbare Ausfälle verursacht durch eingeschleppte Viren, Würmer, etc.
- Neben der Integrität muss für bestimmte Daten auch die Authentizität dieser Datensätze gewährleistet sein, die gegenüber Dritten (z.B. der zuständigen KV) auch nach längerer Zeit nachgewiesen werden können muss. Dies betrifft insbesondere Arrangements in größeren Gemeinschaftspraxen oder auch im Vertretungsfall, da die Frage der Zuordenbarkeit hier sowohl für den einzelnen Arzt als auch für KVen oder Versicherungen von besonderem Interesse ist.
- Die zügige Wiederherstellbarkeit von Daten nach Defekten an Hard- oder Software, oder aber auch nach Fehlbedienung ist zwar nur im Ausnahmefall mit medizinisch ernsthaften Konsequenzen verbunden (z.B. Behandlung von Allergikern), stellt jedoch für die betriebswirtschaftliche Sicherheit einer Praxis einen wichtigen Aspekt dar.

Die o.g. Punkte müssen von Praxis-Informationssystemen geleistet werden. Dabei ist insbesondere zu berücksichtigen, dass die primären Nutzer dieser Systeme meist nicht dazu qualifiziert sind, den Grad der Erfüllung der genannten Krite-

Med-CAST-Forum 2003: IT-Sicherheit in der Medizin

Das Gesundheits- und Sozialwesen in Deutschland steht seit geraumer Zeit vor der Herausforderung, wachsende Möglichkeiten und Anforderungen in Richtung der Verbesserung von Qualität und Effizienz der Versorgung einerseits und sinkende Budgets andererseits, im Sinne einer zukunftsträchtigen Weiterentwicklung zu harmonisieren. Dabei spielt die Informationstechnologie (IT) eine wesentliche Rolle in der ambulanten, stationären und tertiären Versorgung. Die Stichworte Disease Management, DRG, elektronisches Rezept, Gesundheitspass und Qualitätsmanagement mögen als Beispiel hierfür dienen. Die Nutzung der EDV im Gesundheitswesen kann entscheidend zur Vermeidung von Fehlversorgungen und zur Stärkung der Rolle der Patienten beitragen. Sie birgt aber auch immer die Gefahr des Missbrauchs sensibler Patientendaten. Datenschutz, Datensicherheit und IT-Sicherheit spielen für die Nutzung der Informationstechnologie im Gesundheitswesen eine herausragende Rolle und erlegt allen Betroffenen eine große Verantwortung auf. Gerade die Kommunikation im und zum niedergelassenen Bereich stellt dabei eine besondere Herausforderung dar. Daher wurde der Schwerpunkt des MED-CAST-Forums 2003 auf dieses Thema gelegt. Dr. Matthias Herbst, Gründungsmitglied CAST-Forum (www.castforum.de)

Autoren: Matthias Herbst, Stephen D. Wolthusen
Titel: Empfehlungen zur IT-Sicherheit von Praxis-Systemen
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Ober-Mörlen, Ausgabe 2004
Seite: 204-205

rien zu bewerten, oder gar diese Absicherung selbst durchzuführen.

Die Anforderungen sind daher primär von den Anbietern der IT-Systeme, sowie der die Installation und Betreuung der Systeme vornehmenden System- und Beratungshäuser zu erfüllen.

Um eine Bewertung des Ist-Zustandes vornehmen zu können, sollte daher zunächst eine Auswahl von 3-4 führenden Praxis-IT-Systemen in einer typischen Installation auf die Erfüllung der Sicherheitsanforderungen begutachtet werden und neben der Identifikation von Mängeln an bestehenden Systemen eine vorläufige Bewertung der Kritikalität der Mängel vorgenommen werden.

Mögliche weitere Schritte nach Durchführung dieser Studie könnte die Erstellung eines CCITSE-Schutzprofils für Praxis-IT-Systemen sowie von Konfigurationsrichtlinien für derartige Systeme sein, sowie die Identifikation technischer und organisatorischer Maßnahmen zur Beseitigung vorgefundener Mängel.

Entsprechende Vorschläge wurden bereits an die Entscheider in Politik, Verwaltung und IT-Wirtschaft herangetragen. Eine enge Kooperation mit dem BSI ist vorgesehen.