

# Grundschutz für Praxis-Systeme

Stephen D. Wolthusen

Abteilung Sicherheitstechnologie, Fraunhofer-IGD, Darmstadt  
wolt@igd.fhg.de, 12. August 2003

Selbst in kleinen Praxen und mittleren Gemeinschaftspraxen ist der Einsatz von Informations- und Telekommunikations-Systemen (ITK-Systeme) vielfach zu einer unabdingbaren Arbeitsgrundlage geworden, deren Ausfall oder auch Fehlfunktion zu erheblichen Störungen im Arbeitsablauf sowie zu betriebswirtschaftlichen Problemen führen kann [10].

Die potentiellen Einsatzgebiete reichen dabei von nützlichen, aber ersetzbaren Funktionen wie der Terminverwaltung und Personaleinsatzplanung über betriebswirtschaftlich kritische Funktionen wie etwa das Abrechnungswesen für gesetzliche Krankenkassen bis hin zu kritischen Patientendaten wie etwa Arztbriefen und gespeicherten Diagnosedaten, bei denen eine Verfremdung oder auch nur die zeitweilige Nichtverfügbarkeit Gefahren für Gesundheit und Leben von Patienten haben können.

Insofern ist zu hinterfragen, ob es gerechtfertigt ist, einerseits hohe Anforderungen an Medizinprodukte (wie etwa auch Arbeitsplatzrechner im Praxisbereich) zu stellen, jedoch andererseits in Bezug auf die Sicherheit und Vertrauenswürdigkeit der Praxis-ITK-Systeme eine nur punktuelle Qualitätssicherung zu betreiben.

## 1 Anforderungen

Niedergelassene Ärzte bis hin zu mittleren Gemeinschaftspraxen teilen in Bezug auf ITK-Systeme ähnliche Probleme, wie sie auch in vielen anderen freiberuflichen Unternehmungen oder auch kleinen und mittleren Unternehmen anzutreffen sind.

Diese leiten sich primär aus der geringen Größe der Unternehmen ab, die einerseits bedingen, dass aufgrund ungünstiger Kostenstrukturen eine Zentralisierung von ITK-Kenntnissen und -Diensten kaum realisierbar sind, andererseits jedoch die funktionalen Anforderungen an die ITK-Systeme in einer durchaus im klinischen Umfeld anzutreffenden Komplexität vergleichbar sind.

Dabei sind Anforderungen an die Vertraulichkeit von Patientendaten rechtlich klar begründet; diese erstrecken sich auch über die durch ITK-Techniken neu entstehenden Möglichkeiten zur Datenübermittlung, insbesondere jedoch auch über Verletzungen der Vertraulichkeit, die nicht durch den Arzt oder ihm unterstehende Mitarbeiter unmittelbar verursacht werden, sondern bei denen sich Dritte (gleich, ob gezielt oder nicht) Zugang zu den zu schützenden Daten verschaffen.

Ein weiteres Kriterium, bei dem einerseits ärztliche Sorgfaltspflichten beruhen, andererseits auch ein erhebliches betriebswirtschaftliches Interesse bestehen muss ist die Integrität sowohl von ITK-Systemen selbst als auch von gespeicherten Daten und den damit verbundenen Vorgängen und Abläufen.

Diese Integrität muss für Daten über die gesetzlichen Aufbewahrungsfristen aufrecht erhalten werden, was allerdings bereits aufgrund der technischen Weiterentwicklung eine eigene Herausforderung darstellt; hinzu kommt, dass etwa für in der Diagnostik relevante Daten der Erstellungsweg (d.h. Assoziationen zwischen Datensätzen) möglichst lange nachverfolgbar sein muss, um etwa bei Bekanntwerden von Genauigkeitsproblemen mit gewissen Chargen von Diagnostica eine weitere Untersuchung anordnen zu können.

Primär aus betriebswirtschaftlicher Sicht, aber etwa auch wünschenswert z.B. bei Patientendaten die radiologische Untersuchungsergebnisse beinhalten, ist zudem die Verfügbarkeit und effektive Nutzbarkeit der ITK-Systeme. Dies beinhaltet etwa die korrekte Funktion von Geräten oder auch Betriebssystemen und Praxissoftware.

Neben der häufig anzutreffenden Variante, bei der Praxispersonal in Selbsthilfe versucht, diese Anforderungen abzudecken, besteht dabei noch die Möglichkeit einer Vergabe der Verwaltung der ITK-Systeme der Praxis an einen externen Dienstleister. Sowohl bei der ersten als auch bei der letzten Variante ist jedoch festzuhalten, dass die Verantwortlichen (d.h. niedergelassene Ärzte) selten in der Lage sein werden, Bedrohungen annähernd vollständig erfassen zu können und aufgrund der identifizierten Anforderungen eine Evaluierung der erreichten Dienstgüte und Absicherung vornehmen zu können, mithin daher auch über keinen objektiven Qualitätsmaßstab für Dienstleistungen und Produkte für die Praxis-ITK-Systeme verfügen.

## 2 Bedrohungen und Gegenmaßnahmen

Den im vorherigen Abschnitt genannten Anforderungen sind eine Reihe von Bedrohungen entgegenzusetzen, von denen hier exemplarisch nur einige aufgeführt werden sollen.

Verletzungen von Vertraulichkeit sind zwar seit langem einer der primären Gegenstände der Aufmerksamkeit der IT-Sicherheitsforschung, jedoch sind bewusste Verletzungen im Umfeld niedergelassener Ärzte durch Mitarbeiter als eher unwahrscheinlich anzusehen, da davon auszugehen ist, dass organisatorische und persönliche Kontrolle sowie Erwartungshaltungen in einem derartigen Umfeld diesen wirkungsvoller entgegenzutreten als es vertretbare technische Maßnahmen leisten können. Insofern sind einfache Zugriffskontrollmechanismen, die identifizierten und authentisierten Berechtigten den Zugang zu Daten gewährleisten für diesen Zweck ausreichend anzusehen. Anders jedoch sind Bedrohungen durch Dritte anzusehen. Diese Dritte gehen nicht notwendig gezielt gegen das Praxis-ITK-System vor, sondern sind im Bereich von Computerviren, -würmern, und anderen automatisierten Angriffen (dies kann etwa auch über von eventuell vorhandenen Netzwerkverbindungen auch über Einwahlmöglichkeiten für Wartungszwecke geschehen, die von Anbietern von Praxissoftware häufig eingerichtet werden) zu suchen, die über vielfältige Verbreitungswege von Email über Dokumente populärer Standardprogramme bis hin zu Angriffen auf Netzwerkverbindungen (auch transitiver Art) zu sehen. Eine Reihe von Malware-Programmen jüngerer Vergangenheit beinhalten etwa Schadroutinen, die beliebige Dokumente an Dritte (zum Teil zufällig ausgewählt) versenden.

Anders als bei Bedrohungen der Vertraulichkeit muss für Bedrohungen von Daten- und Systemintegritätsverletzungen neben derartigen externen Bedrohungen auch berücksichtigt werden, dass Fehlbedienungen und auch Fehler in den ITK-Systemen selbst erhebliche Teile des Potentials ausmachen. Neben der korrekten Auswahl von robusten und ergonomischen Komponenten [7] zur Reduktion dieses Bedrohungspotentials muss der Datensicherung und Wiederherstellung des Regelbetriebes nach Integritätsverletzung, aber auch Mechanismen zur Erkennung dieser Verletzungen besondere Aufmerksamkeit gelten.

Letzteres kann etwa auch dadurch verursacht werden, dass Datenbestände, die mit älteren Versionen von Programmen erstellt wurden, von neueren Versionen anders interpretiert oder auch nur dargestellt werden, z.B. bei numerischen Daten. Es ist daher unabdingbar, insbesondere jedwede Konfigurationsänderungen an ITK-Systemen exakt nachvollziehbar zu gestalten und zumindestens Kernfunktionen auf die Einhaltung von Erwartungswerten hin zu überprüfen.

Kernelemente einer Sicherheitsarchitektur, die wirkungsvoll die Integrität des ITK-Systems (und damit teilweise auch Vertraulichkeit) sicherstellt, sind daher wirkungsvolle Revisionsmechanismen, Datensicherung, und Kommunikations- und Netzwerksicherheitsverfahren.

Bedrohungen der Verfügbarkeit gehen mittelbar aus den beiden zuvor genannten Bedrohungsfeldern hervor, aber auch physische Gefahrenmomente wie etwa durch Feuer- und Wasserschäden. Auch hier sind Datensicherungen (etwa auch die regelmäßige räumliche Auslagerung wichtiger Datensicherungsbestände, z.B. um die gleichzeitige Vernichtung von Originaldaten und Datensicherung durch Brandschäden zu vermeiden) primäres Werkzeug, um Bedrohungen entgegenzutreten zu können. Anders als im klinischen Umfeld werden jedoch selten neben betriebswirtschaftlichen Aspekten präzise Anforderungen an die Verfügbarkeit zu stellen sein und entsprechend weniger anspruchsvolle und aufwändige Notfallplanungen erforderlich sein...

#### Dokumentinformationen zum Volltext-Download

Ä

Titel:

Grundschutz für Praxis-Systeme

Artikel ist erschienen in:

Telemedizinführer Deutschland, Ausgabe 2004

Kontakt/Autor(en): Stephen D. Wolthusen

Abteilung Sicherheitstechnologie, Fraunhofer-IGD, Darmstadt

wolt@igd.fhg.de, 12. August 2003

Seitenzahl:

4,5

Sonstiges

1 Abb. Dateityp/ -größe: PDF / 196 kB Click&Buy-Preis in Euro: kostenlos

Ä

Rechtlicher Hinweis:

Ein Herunterladen des Dokuments ist ausschließlich zum persönlichen Gebrauch erlaubt. Jede Art der

Weiterverbreitung oder Weiterverarbeitung ist untersagt. Â  
Hier gehts zum freien PDF Download...