Grundschutz fÃ¼r 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 StÃ¶rungen imArbeitsablauf sowie zu betriebswirtschaftlichen Problemen fÃ¼hren kann [10].

Die potentiellen Einsatzgebiete reichen dabei von nÃ¼tzlichen, aber ersetzbaren Funktionen wie der Terminverwaltung und Personaleinsatzplanung Ã¼ber betriebswirtschaftlich kritische Funktionen wie etwa das Abrechnungswesen fÃ¼r gesetzliche Krankenkassen bis hin zu kritischen Patientendaten wie etwa Arztbriefen und gespeicherten Diagnosedaten, bei denen eine Verfremdung oder auch nur die zeitweilige NichtverfÃ¼gbarkeit Gefahren fÃ¼r Gesundheit und Leben von Patienten haben kÃ¶nnen.

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 VertrauenswÃ¼rdigkeit der Praxis- ITK-Systeme eine nur punktuelle QualitÃ¤tssicherung zu betreiben.

1 Anforderungen

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

Diese leiten sich primÃ¤r aus der geringen GrÃ¶ÃŸe der Unternehmen ab, die einerseits bedingen, dass aufgrund ungÃ¼nstiger Kostenstrukturen eine Zentralisierung von ITK-Kenntnissen und -Diensten kaum realisierbar sind, andererseits jedoch die funktionalen Anforderungen an die ITKSysteme in einer durchaus im klinischen Umfeld anzutreffenden KomplexitÃ¤t vergleichbar sind.

Dabei sind Anforderungen an die Vertraulichkeit von Patientendaten rechtlich klar begrÃ¼ndet; diese erstrecken sich auch Ã¼ber die durch ITK-Techniken neu entstehenden MÃ¶glichkeiten zur DatenÃ¼bermittlung, insbesondere jedoch auch Ã¼ber 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 schÃ¼tzenden Daten verschaffen.

Ein weiteres Kriterium, bei dem einerseits Ã¤rztliche Sorgfaltspflichten berÃ¼hrt sind, andererseits auch ein erhebliches betriebswirtschaftliches Interesse bestehen muss ist die IntegritÃ¤t sowohl von ITKSystemen selbst als auch von gespeicherten Daten und den damit verbundenen VorgÃ¤ngen und AblÃ¤ufen.

Diese IntegritÃ¤t muss fÃ¼r Daten Ã¼ber die gesetzlichen Aufbewahrungsfristen aufrecht erhalten werden, was allerdings bereits aufgrund der technischen Weiterentwicklung eine eigene Herausforderung darstellt; hinzu kommt, dass etwa fÃ¼r in der Diagnostik relevante Daten der Erstellungsweg (d.h. Assoziationen zwischen DatensÃ¤tzen) mÃ¶glichst lange nachverfolgbar sein muss, um etwa bei Bekanntwerden von Genauigkeitsproblemen mit gewissen Chargen von Diagnostica eine weitere Untersuchung anordnen zu kÃ¶nnen.

PrimÃ¤r aus betriebswirtschaftlicher Sicht, aber etwa auch wÃ¼nschenswert z.B. bei Patientendaten die radiologische Untersuchungsergebnisse beinhalten, ist zuden die VerfÃ¼gbarkeit und effektive Nutzbarkeit der ITK-Systeme. Dies beinhaltet etwa die korrekte Funktion von GerÃ¤ten oder auch Betriebssystemen und Praxissoftware.

Neben der hÃ¤ufig anzutreffenden Variante, bei der Praxispersonal in Selbsthilfe versucht, diese Anforderungen abzudecken, besteht dabei noch die MÃ¶glichkeit einer Vergabe der Verwaltung der ITKSysteme 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 Ã„rzte) selten in der Lage sein werden, Bedrohungen annÃ¤hernd vollstÃ¤ndig erfassen zu kÃ¶nnen und aufgrund der identifizierten Anforderungen eine Evaluierung der erreichten DienstgÃ¼te und Absicherung vornehmen zu kÃ¶nnen, mithin daher auch Ã¼ber keinen objektiven QualitÃ¤tsmaÃŸstab fÃ¼r Dienstleistungen und Produkte fÃ¼r die Praxis-ITK-Systeme verfÃ¼gen.

2 Bedrohungen und GegenmaÃŸnahmen

Den im vorherigen Abschnitt genannten Anforderungen sind eine Reihe von Bedrohungen entgegenzusetzen, von denen hier exemplarisch nur einige aufgefÃ¼hrt werden sollen.

Verletzungen von Vertraulichkeit sind zwar seit langem einer der primÃ¤ren GegenstÃ¤nde der Aufmerksamkeit der IT-Sicherheitsforschung, jedoch sind bewuÃŸte Verletzungen im Umfeld niedergelassener Ã¤rzte durch Mitarbeiter als eher unwahrscheinlich anzusehen, da davon auszugehen ist, dass organisatorische und persÃ¶nliche Kontrolle sowie Erwartungshaltungen in einem derartigen Umfeld diesen wirkungsvoller entgegentreten als es vertretbare technische MaÃŸnahmen leisten kÃ¶nnen. Insofern sind einfache Zugriffskontrollmechanismen, die identifizierten und authentisierten Berechtigten den Zugang zu Daten gewÃ¤hren fÃ¼r diesen Zweals ausreichend anzusehen. Anders jedoch sind Bedrohungen durch Dritte anzusehen. Diese Dritte gehen nicht notwendig gezielt gegen das Praxis-ITKSystem vor, sondern sind im Bereich von Computerviren, -WÃ¼rmern, und anderen automatisierten Angriffen (dies kann etwa auch Ã¼ber von eventuell vorhandenen Netzwerkverbindungen auch Ã¼ber EinwahlmÃ¶glichkeiten fÃ¼r Wartungszwecke geschehen, die von Anbietern von Praxissoftware hÃ¤ufig eingerichtet werden) zu suchen, die Ã¼ber vielfÃ¤ltige Verbreitungswege von Email Ã¼ber Dokumente populÃ¤rer Standardprogramme bis hin zu Angriffen auf Netzwerkverbindungen (auch transitiver Art) zu sehen. Eine Reihe von Malware-Programmen jÃ¼ngerer Vergangenheit beinhalten etwa Schadroutinen, die beliebige Dokumente an Dritte (zum Teil zufÃ¤llig ausgewÃ¤hlt) versenden.

Anders als bei Bedrohungen der Vertraulichkeit muss fÃ¼r Bedrohungen von Daten- und SystemintegritÃ¤tsverletzungen neben derartigen externen Bedrohungen auch berÃ¼cksichtigt 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 IntegritÃ¤tsverletzung, aber auch Mechanismen zur Erkennung dieser Verletzungen besondere Aufmerksamkeit gelten.

Letzteres kann etwa auch dadurch verursacht werden, dass DatenbestÃ¤nde, die mit Ã¤lteren 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 KonfigurationsÃ¤nderungen an ITK-Systemen exakt nachvollziehbar zu gestalten und zumindestens Kernfunktionen auf die Einhaltung von Erwartungswerten hin zuÃ¼berprÃ¼fen.

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

Bedrohungen der VerfÃ¼gbarkeit gehen mittelbar aus den beiden zuvor genannten Bedrohungsfeldern hervor, aber auch physische Gefahrenmomente wie etwa durch Feuer- und WasserschÃ¤den. Auch hier sind Datensicherungen (etwa auch die regelmÃ¤ÃŸige rÃ¤umliche Auslagerung wichtiger DatensicherungsbestÃ¤nde, z.B. um die gleichzeitige Vernichtung von Originaldaten und Datensicherung durch BrandschÃ¤den zu vermeiden) primÃ¤res Werkzeug, um Bedrohungen entgegentreten zu kÃ¶nnen. Anders als im klinischen Umfeld werden jedoch selten neben betriebswirtschaftlichen Aspekten prÃ¤zise Anforderungen an die VerfÃ¼gbarkeit zu stellen sein und entsprechend weniger anspruchsvolle und aufwÃ¤ndige Notfallplanungen erforderlich sein...

Dokumentinformationen zum Volltext-Download
Â
Titel:
Grundschutz fÃ¼r Praxis-Systeme
ArtikelÂ istÂ erschienenÂ in:
TelemedizinfÃ¼hrer 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/ -grÃ¶ÃŸe: PDF /Â Â 196 kBÂ Click&Buy-PreisÂ inÂ Euro: kostenlos

Â