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 imArbeitsablauf 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 berührt sind, 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 zuden 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

Autor: Stephen D. Wolthusen
Titel: Grundschutz für Praxis-Systeme
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Ober-Mörlen, Ausgabe 2004
Seite: 225-229

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 entgegentreten als es vertretbare technische Maßnahmen leisten können. Insofern sind einfache Zugriffskontrollmechanismen, die identifizierten und authentisierten Berechtigten den Zugang zu Daten gewähren für diesen Zweals 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 zuüberprüfen.

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 entgegentreten 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.

3 Status Quo in ITK-Praxissystemen

Bestehende Praxis-ITK-Systeme erfüllen nur selten die hier angeführten Ansprüche; Ursachen hierfür sind jedoch an mehreren Stellen zu identifizieren. Zum einen ist eingeschränktes Problembewußtsein seitens der Betreiber und Kunden (d.h. niedergelassener Ärzte), das meist nur angesichts konkreter Vorfälle Ausprägung findet – ein durchaus nicht bereichsspezifisches Problem, das angesichts der sich schnell ändernden technischen Grundlagen und Bedrohungen als konstant anzusehen ist, da ein nicht realisierbarer Aufwand für eine Verbesserung des Problembewusstseins wäre.

Ein ähnlicher Mangel an Problembewusstsein ist jedoch auch bei Herstellern von Praxissoftware sowie bei Systemhäusern festzustellen, die derartige Praxis-Software zu Systemen konfigurieren und betreuen. Zwar stellen sich diesen Unternehmen dieselben Probleme bei der Verfolgung des Standes der Technik wie den eigentlichen Anwendern, doch fehlt zunächst eine klare betriebswirtschaftliche Motivation, diesen Mangel zu beheben, da die angesprochenen Kunden nur sehr eingeschränkt zwischen ITK-Sicherheit berücksichtigenden und fahrlässig konstruierten Systemen unterscheiden können [1, 6].

Die aus den genannten Defiziten resultierenden Probleme beinhalten unter anderem, dass keine sinnvolle Risikoanalysen für Praxissysteme insgesamt durchgeführt werden, sondern wenn überhaupt punktuelle Lösungen auf Anwendungsebene eingeführt werden, die dann als Leistungsmerkmal auch beworben werden können.

Dabei ist insbesondere festzuhalten, dass derartige Maßnahmen nur dann sinnvoll sind, wenn die Systeminfrastruktur (Netzwerkzugänge, Betriebssystem-Konfiguration, etc.) ihrerseits hinreichend abgesichert ist; entsprechende Vorgaben wären etwa von Herstellern für Komplettsysteme zu erwarten oder im Kompetenzbereich der Praxis-Systeme einrichtenden Systemhäuser anzusiedeln.Werden diese Infrastruktur-Komponenten bei der Risikoanalyse und damit auch bei der Absicherung des Systemes ausgelassen, so ist die Sicherheit des Gesamtsystems sehr leicht zu kompromittieren, da die Annahmen (so vorhanden) der Anwendungsentwickler bezüglich Sicherheitskonfigurationen nicht erfüllt werden können.

4 Der Grundschutz-Begriff

Nicht zuletzt aufgrund des oben genannten Informationsdefizites bei Bedarfsträgern ist es daher sinnvoll, Mindeststandards zu setzen, deren Einhaltung entweder aufgrund von Rechtsvorschriften und Verordnungen oder aber auch aufgrund von Wettbewerbsvorteilen bei Einhaltung der Standards durchsetzbar ist. Hierfür existieren sowohl auf nationaler Ebene [4] als auch international [9] eine Reihe von Standards, die für geringen und mittleren Schutzbedarf Verhaltens-, Organisations- und Konfigurationsregelwerke bereitstellen oder bei deren Erstellung

unmittelbar hilfreich sind. Auf niedrigerer Abstraktionsebene bietet seit längerem etwa die U.S. National Security Agency eine Reihe von Konfigurationshandbüchern für Microsoft Windows NT 4.0 und Windows 2000 [3] der Öffentlichkeit zur Verfügung. Diese ermöglichen mittels detailierter Planungs- und Umsetzungshilfen eine Absicherung der Betriebssysteme und Vernetzung auf einem vertretbaren technischen Niveau der genannten Systeme vorzunehmen.

5 Möglichkeiten zur Qualitätssicherung

Da jedoch Praxis-ITK-Systeme einerseits eine Reihe von Anforderungen aufweisen, die über die in Grundschutzdokumenten behandelten Themen hinausgehen, andererseits jedoch auch gerade die für die korrekte Anwendung der Grundschutzmechanismen erforderliche Bedarfsanalyse und Evaluierung der Umsetzung mit erheblichem Aufwand verbunden ist, ist eine in Anforderungen an Leistungsumfang und Umsetzung spezifischere Lösung, die zudem auch international anerkannt werden kann, eine sinnvolle Ergänzung der allgemeinen Grundschutzmaßnahmen.

Auch hierfür existieren international anerkannte Verfahren, deren Anwendung etwa im öffentlichen Bereich sowohl innerhalb Deutschlands als auch in einer Reihe anderer Länder (z.B. den USA) vorgeschrieben ist, sofern kein zwingender Grund existiert, davon abzusehen.

5.1 Die Common Criteria for Information Technology Security Evaluation

Nach einer Reihe von weltweiten nationalen Bestrebungen sowie Vorarbeiten auf europäischer Ebene wurde mit den Common Criteria for Information Technology Security Evaluation (CCITSE, oft auch CC) [8] ein internationaler Standard geschaffen, welcher die Beschreibung von Sicherheitsmerkmalen und deren Umsetzung in ITK-Systemen abdeckt sowie jeweils Verfahren für die Evaluierung dieser Ansprüche und Realisierungen beschreibt.

Die Ergebnisse derartiger Prüfungen, die jeweils von akkreditierten Prüfstellen oder nationalen Schemata selbst vorgenommen werden, werden dabei aufgrund einer Reihe von internationalen Abkommen weitestgehend wechselseitig in verschiedenen Staaten anerkannt, was für Hersteller eine erhebliche Vergrößerung des Marktpotentials gegenüber rein national angelegten Prüfverfahren darstellt.

5.2 Schutzprofile und Sicherheitsvorgaben

Anders als frühere Bestrebungen, die eher monolithische Kriterienkataloge für sichere Systeme zur Folge hatten [2], sind die CCITSE modular angelegt und sollen daher die komponentenorientierte Zusammenstellung von Systemen ermöglichen.

Die Anforderungen an Produkte und Systeme untergliedern sich in zwei Kategorien. Einerseits werden funktionale Aspekte der Systemsicherheit betrachtet, andererseits auch die Vertrauenswürdigkeit und Zuverlässigkeit, mit der die sicherheitsrelevanten Leistungsmerkmale erbracht werden.

Um gewährleisten zu können, dass Produkte mehrerer Hersteller in der Erfüllung der Sicherheitsanforderungen vergleichbar sind und diese selbst ihrerseits in sich geschlossen und sinnvoll sind, verwenden die CCITSE das Konzept eines Schutzprofils (engl. Protection Profile, PP). Dabei handelt es sich um eine nach formalen Kriterien strukturierte Menge von Anforderungen an ein System oder auch eine Komponente sowie eine Dokumentation der Annahmen wie etwa der Umgebung des Systems[1], unter denen die Sicherheitsmechanismen hinreichend sind (siehe Abbildung 1) [5].

Schutzprofile werden von nationalen Schemata, in Deutschland dem Bundesamt für Sicherheit in der Informationstechnik, geprüft und zertifiziert; ein derartiges Zertifikat sagt allerdings nur aus, dass die im Schutzprofil spezifizierten Sicherheitsanforderungen in sich geschlossen sind und den formalen Anforderungen der CCITSE genügen – nicht jedoch, ob ein Schutzprofil für eine gegebene Aufgabe und Anwendungssituation hinreichend ist.

Ein weiteres wesentliches Merkmal, das die Aussagekraft einer Konformität mit einem Schutzprofil beeinflusst ist der Grad der Vertrauenswürdigkeit (engl. Evaluation Assurance Level, EAL), der angefordert wird. Dieser wird in einer Skala von EAL 1 bis 7 angegeben und bedingt auf Ebene der Schutzprofile eine mit höheren Anforderungsstufen signifikant anwachsende Reihe von Anforderungen an die Entwicklung und Entwicklungsumgebung der

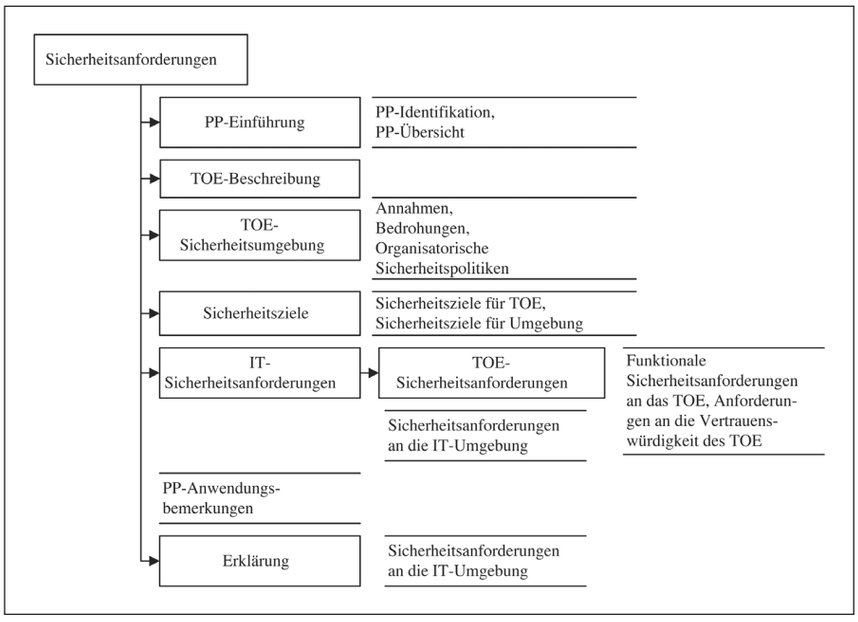

Abbildung 1: *Struktur eines CCITSE-Schutzprofils*

Produkte, um hinreichende Vertrauenswürdigkeit gewährleisten zu können.

Schutzprofile selbst können jedoch nicht als Grundlage für die Entwicklung oder Anpassung von Produkten dienen, da sie noch zu abstrakt gefaßt sind; dieser Detailgrad ist zwar ausreichend für die Bewertung eines Produktes von Seiten eines Anwenders, nicht jedoch für die eigentliche Entwicklung. Um den Schritt hin zu Produktanforderungen durchführen zu können sind weitere Dokumente, die Sicherheitsvorgaben (engl. Security Targets, ST) erforderlich. Diese sind analog zur Darstellung in Abbildung 1 strukturiert, enthalten jedochüber Schutzprofile hinausgehende, für Realisierungen spezifische Anforderungen.

Wie Schutzprofile sind auch Sicherheitsvorgaben zu evaluieren und zertifizieren; es ist dabei durchaus zulässig, Sicherheitsvorgaben direkt zu erstellen und nicht von Schutzprofilen abzuleiten. Nachteil einer derartigen Konstruktion ist jedoch, dass eine solche Sicherheitsvorgabe für genau ein Produkt zutreffend ist, und seitens der Anwender keine Vergleichbarkeit und Transparenz bereitstellt.

Eine alternative Vorgehensweise besteht jedoch darin, aufgrund eines oder mehrerer bestehender Schutzprofile eine Sicherheitsvorgabe zu erstellen; dabei ist darauf zu achten, dass auch die Kombination mehrerer Schutzprofile keine inhaltlichen Lücken aufweisen darf. Dies kann auch dadurch erreicht werden, dass zunächst ein neues Schutzprofil als Kombination bestehender Schutzprofile erstellt und zertifiziert wird.

Für den Anwendungsfall der Praxis-ITK-Systeme ist aufgrund der abzudeckenden Komplexität und Anwendungsanforderungen die zuletzt angerissene Vorgehensweise bei weitem die sinnvollste, da einerseits hierdurch für Anwender ein notwendiges Maß an Transparenz zu erreichen ist, andererseits für Anbieter und Systemhäuser die Möglichkeit besteht, mit vertretbarem Aufwand Kombinationen von Teilkomponenten zusammenzustellen, um die Vorgaben eines solchen Schutzprofils zu erfüllen.

Aufgrund dieser Art erstellter Sicherheitsanforderungen können nun Produkte und Systeme von akkreditierten Prüfstellen evaluiert werden; dabei ist es Aufgabe der Prüfstelle sowohl die funktionalen Anforderungen an die Sicherheit des Systems oder der Komponente zu prüfen sowie die Vertrauenswürdigkeit (je nach Vertrauenswürdigkeitsstufe etwa Güte der Dokumentation, Entwicklungsprozesse, Vorgehensweise bei Auslieferung, Inbetriebnahme, und Wartung).

Analog zu den Zertifikaten für Schutzprofile und Sicherheitsanforderungen werden für erfolgreich durchgeführte Evaluierungen von nationalen Schemata Zertifikate vergeben, die im Regelfall über wechselseitige Anerkennungsverfahren auch international Gültigkeit haben.

6 Zertifizierung von Praxis-ITK-Systemen

Die Erstellung von Schutzprofilen für Praxis-ITK-Systemen (hierbei kann es sich durchaus auch um eine abgestufte Familie von Schutzprofilen handeln, die verschiedenen Anforderungsstufen besser gerecht werden können als ein Profil, das maximale Anforderungen stellt) und die Einführung der Forderung nach zertifizierten Systemen als Regelanforderung bietet daher für das Gesundheitswesen, insbesondere jedoch aber für einzelne niedergelassene Ärzte erhebliche Vorteile.

Zum einen bietet ein nach einem anerkannten Schutzprofil evaluiertes System einen objektiven Vergleichsmaßstab, um Produkte bewerten zu können. Um die Anwendbarkeit und Relevanz der Schutzprofile sicherzustellen sind diese von den Beteiligten im Gesundheitswesen gemeinsam zu erstellen, da etwa Anforderungen bezüglich Schnittstellen zwischen verschiedenen DV-Systemen und den rechtmäßig zuübermittelnden Daten die Interessen mehrerer Beteiligter berühren und diese zudem datenschutzrechtlich validiert werden müssen.

Zum anderen bieten zu Schutzprofilen konform erstellte und installierte Produkte einen Mindestmaß für die Qualität und Betriebssicherheit von Installationen, die auch von externen Gutachtern im Rahmen von Abnahmevorgängen oder auch Nachevaluierungen im Zuge von Qualitätssicherungsmaßnahmen bewertet werden können.

Dies ist insbesondere deswegen sinnvoll, da anders als in dem im Grundschutzbereich [4, 9] angenommenen Fall in Praxis-ITK-Systemen es sich mit geringen Variationen nicht um stark anwendungsspezifische Situationen handelt, die in einem vergleichsweise umfangreichen Prozeß individuell modelliert und in ihren Sicherheitsmechanismen angepasst werden müssen, sondern vielmehr um Systeme, die durch stark strukturierte Vorgaben gut abgedeckt werden können; dies hat einerseits für den einzelnen niedergelassenen Arzt erhebliche Kostenvorteile, da nur begrenzt Individualdienstleistungen in Anspruch genommen werdenmüssen, und reduziert andererseits die Möglichkeiten für Kompromittierungen der ITK-Systeme durch Fehlkonfigurationen oder unzulässige Einsatzgebiete.

Das hier angerissene Vorgehen weist jedoch auch eine Reihe von Nachteilen auf, die hier ebenfalls kurz dargestellt werden sollen. Zunächst fallen sowohl für die Erstellung von Schutzprofilen und Sicherheitsanforderungen bei Erstellung und Evaluierung Kosten an, die zudem mit Verzögerungen durch die Evaluierung und, je nach gewünschter Vertrauenswürdigkeitsstufe, Änderungen in Entwicklungsprozessen (d.h. Konfigurationsmanagement, Anforderungen an Dokumentation und Spezifikation von Komponenten) zur Folge haben.

Ähnliches gilt auch für die Entwicklung und Evaluierung der Produkte selbst, da auch hier in Abhängigkeit der in Schutzprofilen und Sicherheitsanforderungen festgelegten Anforderungen erhebliche Aufwände anfallen können. Insbesondere für die Spezifikation und Bereitstellung kompletter Praxis-ITK-Systeme ist dabei auch die Verfolgung von Konfigurations änderungen von hoher Bedeutung, da anderenfalls ein zertifiziertes Produkt nur sehr kurze Zeit marktrelevant sein kann, etwa weil erforderliche Komponenten von Zulieferern nicht mehr angeboten werden.

Dennoch stellt die Einführung der hier dargestellten Qualitätssicherungsmaßnahmen einen wesentlichen Beitrag dar, um die zunehmende Abhängigkeit von ITK-Systemen auch im Anwendungsbereich niedergelassener Ärzte durch Verbesserungen der Qualität und Sicherstellung gleichbleibender und objektiver Maßstäbe für die Bewertung dieser flankieren zu können.

Literatur

[1] AKERLOF, G. A. The Market for "Lemons": Quality Uncertainty and the Market Mechanism. The Quarterly Journal of Economics 84, 3 (Aug. 1970), 488–500.

[2] ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE. DoD 5200.28-STD: Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC). United States Department of Defense, 1985.

[3] BARTOCK, P. F., ET AL. Security Recommendation Guides. United States National Security Agency, 2003. 21 Teile.

[4] BUNDESAMT FüR SICHERHEIT IN DER INFORMATIONSTECHNIK. ITGrundschutzhandbuch. Bundesanzeiger-Verlag, Bonn, 2002. 14

[5] BUSCH, C., AND WOLTHUSEN, S. D. Netzwerksicherheit. Spektrum Akademischer Verlag, Heidelberg, Germany, 2002.

[6] DEKEL, E., AND SCOTCHMER, S. On the Evolution of Attitudes toward Risk in Winner-Take-All Games. Journal of Economic Theory 87, 1 (Jan. 1999), 125–143.

[7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Ergonomic Requirements for Office Work with Visual Display Terminals – International Standard 9241. ISO, 1997. 17 Teile.

[8] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION AND INTERNATIONAL ELECTROTECHNICAL COMMITTEE. Common Criteria for Information Technology Security Evaluation – International Standard 15408. ISO, 1999. Version 2.1.

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION AND INTERNATIONAL ELECTROTECHNICAL COMMITTEE. Information Technology – Code of Practice for Information Security Management. International Standard 17799. ISO, 2000.

[10] LEVESON, N. G. Safeware: System Safety and Computers. Addison-Wesley, Reading, MA, USA, 1995. 15

Fußnote

1 auch TOE, Target of Evaluation oder EVG, Evaluierungsgegenstand genannt