Marcel Winandy

Informationssicherheit in der Arztpraxis: Aktuelle Herausforderungen und Lösungsansätze

Eine wachsende Vernetzung der IT-Systeme im Gesundheitswesen verspricht eine effizientere Abwicklung von Dienstleistungen. Während Sicherheitsanforderungen und Sicherheitsarchitekturen für die Netzinfrastrukturen oft sehr umfassend sind, werden die Computerarbeitsplätze in den Arztpraxen häufig einfach nur als vertrauenswürdig angenommen bzw. in der Verantwortung der jeweiligen Arztpraxis gesehen. Doch ist das eine realistische Annahme? Welche Aspekte spielen eine Rolle?

Einleitung

Die zunehmende Digitalisierung macht auch vor dem Gesundheitswesen nicht halt. Während sie zum einen viele neue Vorteile bietet, z.B. Behandlungen effektiver und effizienter machen kann, birgt sie zum anderen auch gewisse Risiken und Herausforderungen. Die Komplexität heutiger IT-Systeme und deren Vernetzung macht es nicht immer einfach, alle Anforderungen des Datenschutzes und der Datensicherheit ohne weiteres zu realisieren. Gerade unter diesem Gesichtspunkt ist die Betrachtung der Informationssicherheit im Gesundheitswesen besonders wichtig, da es um äußerst sensitive Daten geht: die medizinischen Daten von Patienten.

Diverse Anwendungen für „electronic Health“ (eHealth) Systeme sind von Industrie und Politik geplant, manche sind bereits im praktischen Einsatz. Während die derzeit verfügbaren Anwendungen im Kontext der elektronischen Gesundheitskarte (eGK) sich nur auf Versichertenstammdaten und die Integration der Europäischen Krankenversicherungskarte auf der eGK beschränken (weitere Anwendungen sind „in Vorbereitung“) [1], gibt es andernorts bereits elektronischen Datenaustausch für bestimmte Anwendungen. Darunter zählt neben der Elektronischen Fallakte (EFA) [2] auch das Netz der Abrechnungssysteme der Kassenärztlichen Vereinigungen (KV-SafeNet) [3]. Letzteres ermöglichst es den niedergelassenen Ärzten, ihre erbrachten Leistungen online über ein spezielles Netzwerk mit den Kassenärztlichen Vereinigungen (KVen) abzurechnen, die wiederum die Abrechnung mit den Gesetzlichen Krankenkassen vornehmen.

Dieser Artikel beleuchtet die dahinterstehenden Sicherheitsarchitekturen. Insbesondere wird ein Blick auf die Rolle der Primärsysteme geworfen, d.h. der lokalen IT-Infrastruktur in der Arztpraxis. Diese werden nämlich oft nicht genauer betrachtet, bzw. als sicher angenommen. Mit anderen Worten: Die Informationssicherheit der Arztpraxis fällt nicht in den Zuständigkeitsbereich der eHealth-Sicherheitsarchitektur.

Es soll hier der Frage nachgegangen werden, wie man die Vertraulichkeit und Integrität eines IT-Systems in der Arztpraxis sicherstellen kann. Ist das überhaupt ein realistisches (oder realisierbares) Ziel? Größere Institutionen wie Krankenhäuser können sich ggf. eine eigene IT-Abteilung leisten. Niedergelassene Ärzte managen ihre IT-Systeme oft selbst. Es ist eine weitere Herausforderung, dass dieselben IT-Systeme oft für unterschiedliche Anwendungen gleichzeitig genutzt werden.

Im folgenden wird ein allgemeines Grundmodell für eHealth-Architekturen beschrieben und am Beispiel des KV-SafeNet analysiert, welche Probleme und Herausforderungen es bei der Informationssicherheit in der Arztpraxis gibt. Anschließend werden generelle Lösungsansätze diskutiert und exemplarisch ein konkreter Ansatz aus einem aktuellen Forschungs- und Entwicklungsprojekt beschrieben.

Grundmodell einer eHealth-Architektur

Es gibt verschiedene Ausformungen von eHealth-Architekturen: zum Beispiel die Anbindung an das Netzwerk der Kassenärztlichen Vereinigungen (KV-SafeNet) [3], die Telematikinfrastruktur der elektronischen Gesundheitskarte (eGK) [1] in Deutschland sowie diverse Formen einrichtungsübergreifender Elektronischer Patientenakten in anderen Ländern. Allen diesen Architekturen ist jedoch ein Grundmodell oft gemeinsam: Primärsysteme der Leistungserbringer (z.B. Arzt-PC) werden über spezielle Verbindungselemente (VPN-Box) in ein abgeschirmtes Kommunikationsnetz angeschlossen, in dem verschiedene eHealth-Dienste als Fachanwendungen online erreichbar sind (z.B. Abrechungssysteme, elektronischer Arztbrief, Elektronische Patientenakten).

Aus Gründen der Wirtschaftlichkeit werden die Verbindungen in die eHealth-Dienste-Infrastruktur über vorhandene Internet-Anschlüsse realisiert. Um Vertraulichkeit und Integrität der Datenübertragung dabei zu gewährleisten, greift man auf vorhandene Sicherheitstechnologien wie Virtuelle Private Netze (VPN) zurück. Ein solches VPN kann einen sicheren Kanal durch nicht-vertrauenswürdige Netze wie dem Internet aufbauen. Dabei wird die gesamte Kommunikation zwischen den End-

Marcel Winandy
Wissenschaftlicher Mitarbeiter (PostDoc) in der Forschungsgruppe Systemsicherheit der Ruhr-Universität Bochum, Projektkoordinator für Projekte zu IT-Sicherheit von eHealth-Systemen

marcel.winandy@trust.rub.de

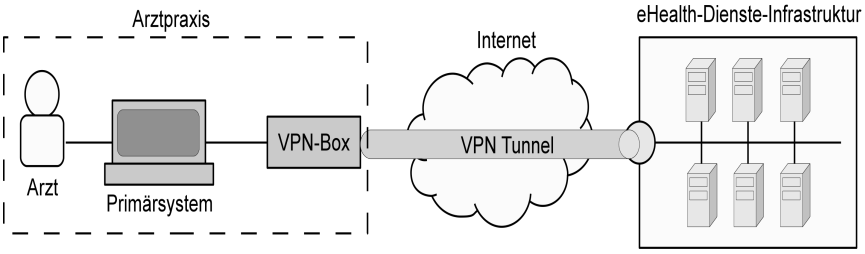

Abb. 1: Grundmodell eHealth-Architektur

punkten (Primärsystem bzw. eHealth-Dienste-Infrastruktur) auf Netzwerkebene verschlüsselt und gegen unbemerkte Integritätsverletzungen geschützt.

Das Grundmodell solcher eHealth-Architekturen enthält drei wesentliche Elemente, die für die Sicherheitsbetrachtung relevant sind (siehe Abb. 1):

- **Primärsystem**
  Die Computerplattformen eines Leistungserbringers werden als Primärsystem bezeichnet. Dies umfasst logisch sowohl einzelne Rechner als auch komplette lokale Netzwerkinfrastrukturen, z.B. das WLAN einer Arztpraxis. In den Primärsystemen werden Daten von Patienten erfasst, verarbeitet und an andere Teile der eHealth-Architektur weitergeleitet bzw. von dort bezogen. Dies können medizinische Daten für eine Elektronische Patientenakte sein (wie es zukünftig geplant ist), oder Daten für die Abrechnung mit den Kassenärztlichen Vereinigungen (wie es derzeit bereits im Rahmen von KV-SafeNet praktiziert wird).
- **Verbindungselement (VPN-Box)**
  Um über das Internet sicher an die interne eHealth-Architektur zu gelangen, gibt es typischerweise ein dediziertes Verbindungselement in der Arztpraxis. Dies ist oft eine kleine Hardware-Box, die eine verschlüsselte VPN-Verbindung in die abgeschirmte Kommunikationsinfrastruktur der eHealth-Dienste aufbaut. Die VPN-Box enthält dazu die notwendigen kryptographischen Zertifikate und zugehöriges Schlüsselmaterial. Ein wichtiger Aspekt hierbei ist der Schutz gegen Ausspähen oder Manipulation des geheimen Schlüsselmaterials. Dazu wird üblicherweise auf den Einsatz eines Hardware-Sicherheitsmoduls, z.B. in Form einer Chipkarte, zurückgegriffen. Beispiele für solche VPN-Boxen sind der „Konnektor“ bei der Telematikinfrastruktur der eGK oder der „KV-SafeNet-Router“ bei der Abrechnungsinfrastruktur der KVen. Allerdings nur die Spezifikation des Konnektors fordert explizit den Einsatz eines Sicherheitsmoduls zum Schutz des Schlüsselmaterials [4].
- **eHealth-Dienste-Infrastruktur**
  Das Herzstück einer eHealth-Architektur ist schließlich die innere Kommunikationsinfrastruktur, die in einem abgeschirmten Netz (ähnlich wie einen Unternehmens-Intranet) realisiert ist. In dieser Infrastruktur können verschiedene Dienste verfügbar sein. Einige dieser Dienste arbeiten dabei mit patientenbezogenen Daten, z.B. Abrechungssysteme oder Elektronische Patientenakten. Die Sicherheit (Vertraulichkeit und Integrität der Daten) dieser Infrastruktur beruht hauptsächlich darin, dass der Zugang nur über ein entsprechendes Verbindungselement (VPN-Box) von außen möglich ist. Innerhalb dieser Infrastruktur können jedoch auch weitere Sicherheitsmechanismen für einzelne Dienste greifen (Zugriffskontrolle, Verschlüsselung der Datenspeicherung, Protokollierung von Zugriffsversuchen, etc.).

Vertrauensmodell

Die meisten Ausgestaltungen des beschriebenen Grundmodells, insbesondere die Telematikinfrastruktur und das KV-SafeNet, definieren klare Vorgaben für die Sicherheitseigenschaften der eHealth-Dienste-Infrastruktur und des Verbindungselements (VPN-Box).

Die eHealth-Dienste-Infrastruktur an sich wird bei näherer Betrachtung prinzipiell als vertrauenswürdig angenommen. Das bedeutet, dass nur der Zugang von außen abgesichert werden muss. Die Vertraulichkeit und Integrität der Dienste-Infrastruktur intern wird oft einfach angenommen. Die KVen sprechen hier von einem „sicheren Netz“ [3].

Die VPN-Box wird ebenfalls als vertrauenswürdig betrachtet. Im Falle der Telematikinfrastruktur gibt es für den Konnektor jedoch genaue Sicherheitsvorgaben in Form eines Common Criteria Schutzprofils [4]. Der KV-SafeNet-Router sollte auch nach Common Criteria evaluiert sein (Empfehlung gemäß [5]), allerdings findet sich keine Angabe nach welchem Schutzprofil.

Schließlich werden auch die Primärsysteme als vertrauenswürdig angenommen. Weder bei der Telematikinfrastruktur noch bei KV-SafeNet werden explizite Spezifikationen zu den Endsystemen der Ärzte definiert [7][9]. Lediglich allgemeine Vorgaben und Empfehlungen werden ausgesprochen, wie z.B. der Betrieb von Antimalwareprogrammen und regelmäßigen Softwareaktualisierungen [7]. Allerdings gibt es weder technische Überprüfungen, ob diese Maßnahmen auch eingesetzt werden, noch eine Garantie für deren Effektivität (Updates können wieder neue Fehler einführen, und Virenscanner erkennen nicht alle Schadprogramme). Aus Sicht der Gesamtarchitektur bleibt somit die Annahme der Vertrauenswürdigkeit.

Vertraulichkeit und Integrität der IT in der Arztpraxis

Die IT-Systeme in Arztpraxen bearbeiten Daten mit hohem Schutzbedarf, insbesondere medizinische Daten von Patienten. Der Schutz der Vertraulichkeit und Integrität dieser Daten steht dabei im Vordergrund. Die Vertraulichkeit muss gewährleistet sein, um nicht nur der ärztlichen Schweigepflicht Genüge zu tun, sondern um auch allgemein den Datenschutz der personenbezogenen Daten der Patienten zu sichern. Ebenso muss sich ein Arzt darauf verlassen können, dass abgerufene und abgespeicherte medizinische Daten nicht unautorisiert verändert wurden, d.h. dass ihre Integrität gewährleistet ist. In bestimmten Fällen kann auch die Verfügbarkeit ein Schutzziel sein. Im allgemeinen kann jedoch bei Nichtverfügbarkeit eine Diagnose erneut gestellt werden, während eine Behandlung aufgrund von falschen Daten schwerwiegendere Konsequenzen nach sich zieht.

Im folgenden gehen wir davon aus, dass die eHealth-Dienste-Infrastruktur und die VPN-Verbindung durch die entsprechende VPN-Box sicher sind, d.h. die Vertraulichkeit und Integrität aller dort kommunizierten Daten gewährleistet wird.

Wir negieren an dieser Stelle allerdings die übliche Annahme, dass die Primärsysteme der Leistungserbringer „sicher“ sind. Faktisch sind nämlich die technischen Voraussetzungen oft gar nicht gegeben, um diese Annahme als realistisch zu betrachten. Primärsysteme

sind normalerweise handelsübliche PCs mit Standardbetriebssystemen, d.h. mit all ihren architekturbedingten Schwächen in Sachen Informationssicherheit. Hinzu kommt, dass insbesondere kleinere Arzthäuser und Arztpraxen sich keinen professionellen IT-Administrator leisten können (oftmals ist es der Arzt selbst oder dessen Sohn oder Nachbar).

Manche Produktbeschreibungen versprechen zwar eine einfache und „absolut sichere" Konfiguration, die Realität sieht oft jedoch anders aus. So heißt es z.B. in einem Informationsblatt der KBV [3]: *„Medizinische Daten erfordern besonderen Schutz. KV-SafeNet bietet ihn. Und das Beste: Sie benötigen nur einen internetfähigen Computer, einen Internetanschluss und einen Router."* Bei genauerer Betrachtung der Spezifikationen [7] findet sich dagegen diese Aussage: *„Der Arzt trägt die Verantwortung für Sicherheit seiner Praxis-IT und für den Schutz der Patientendaten."* Hier wird also die Verantwortung wieder auf die Arztpraxis abgewälzt.

Aber wo genau liegt das Problem? Im allgemeinen Grundmodell schützt die VPN-Box als sicheres Verbindungselement den Zugang zu den eHealth-Diensten und damit die Patientendaten. Allerdings ist die Praxis-IT oft nicht nur mit diesem einem „sicheren Netz" verbunden, sondern ggf. auch mit anderen Netzen oder direkt mit Diensten aus dem Internet (z.B. E-Mail oder Webbrowser für Recherche-Zwecke). Dies bedeutet im Zweifelsfall, dass die Praxis-IT Bedrohungen durch Schadsoftware und Angriffen aus dem Internet ausgesetzt ist. Allerdings kann diesem Bedrohungsszenario nicht allein durch Firewalls begegnet werden. Eine Firewall kann den aktuellen Netzwerkverkehr beschränken, sie hat jedoch keinen Einfluss auf oder Kontrolle über die ausgeführten Programme in der Praxis-IT.

Auf den Rechnern der Praxis-IT werden typischerweise mehrere verschiedene Anwendungen ausgeführt, ggf. mit jeweils unterschiedlichem Schutzniveau basierend auf den Daten, mit denen sie arbeiten. Programme, die nichts mit Patientendaten zu tun haben, sollten auch keinen Zugriff darauf haben. Wie allerdings die interne Arbeitsweise der Praxis-IT und deren Software-Konfiguration ist, kann die VPN-Box weder bestimmen noch kontrollieren.

Kritisch wird die beschriebene Situation, wenn aus der Praxis-IT heraus einmal Patientendaten zu eHealth-Diensten geschickt werden (z.B. Abrechnungsdaten an die KVen) und zu einem anderen (früheren oder späteren) Zeitpunkt Dienste aus dem Internet abgerufen werden (z.B. für ein Software-Update). Letzteres kann dazu führen, dass Software-Programme, die auf derselben Praxis-IT (z.B. auf einem Arzt-PC) ausgeführt werden, die Vertraulichkeit verletzen können, wenn sie bei einer Internet-Verbindung Patientendaten an ein unautorisiertes Ziel schicken. Die Integrität der Daten oder vorhandener Programme kann ebenfalls auf diese Art verletzt werden. Eine VPN-Box, die beim Aufbau des VPN-Tunnels in die eHealth-Dienste-Infrastruktur jeglichen Verkehr aus dem Internet in die Praxis-IT und umgekehrt blockiert, schützt nur in diesem Moment. Wenn zu einem anderen Zeitpunkt Dienste im Internet aufgerufen werden (z.B. wenn der VPN-Tunnel nicht aktiv ist), können sich Schadprogramme in die Praxis-IT „einnisten" und später (wenn der VPN-Tunnel wieder aktiv ist) auch das „sichere Netz" der eHealth-Dienste-Infrastruktur von innen heraus befallen.

Neben der Bedrohung durch Schadsoftware kann auch der externe Zugriff durch Fernwartung von Software-Programmen problematisch sein: Der Software-Hersteller darf im Rahmen der Fernwartung keinen Zugriff auf Patientendaten erhalten! Während rechtlich der Fall klar ist, bleibt die Frage nach entsprechenden technischen Vorkehrungen.

Das Szenario „eHealth-Dienste-Netz und Internet" ist auch im Kontext von KV-SafeNet bekannt und wird als Szenario mit „sehr großem Angriffspotential" beschrieben [7]. Eine Lösung wird jedoch nicht gegeben. Dort heißt es nur, der KV-SafeNet-Router *„baut ein virtuelles privates Netzwerk (VPN) zu einem Einwahlknoten in der KV auf, welches die Verbindung vom normalen Internet abschottet. [...] Gleichzeitig blockiert der Router den Zugriff von außen auf das Praxis-Netzwerk und die dortigen Daten"* [5]. Dass der KV-SafeNet-Router zudem als „Black Box" arbeitet und nur der Hersteller dessen genaue Konfiguration kennt, wurde an anderer Stelle bereits kritisiert [8].

Schadsoftware kann zudem auch über andere Wege auf die Praxis-IT gelangen, z.B. durch unautorisierte oder gefälschte Software-Updates und schließlich auch über das Einspielen von externen Datenträgern (z.B. USB-Sticks).

Zu guter Letzt, selbst wenn durch technische Vorkehrungen jegliche Schadsoftware vermieden werden könnte, bleibt die Gefahr von Fehlkonfigurationen oder Fehlbedienungen, die ebenfalls zu einer Verletzung der Integrität und Vertraulichkeit führen können. Ein einfaches Beispiel: Ein Dokument mit medizinischen Daten eines Patienten wird irrtümlicherweise über die Betriebssystemoberfläche auf einen falschen Ordner „geschoben", der zu einem externen Datenträger (Netzlaufwerk oder USB-Stick) gehört. Das Speichern sensitiver Daten auf externe Datenträger entgeht jeglicher Kontrolle durch Netzwerk-Firewalls. Wenn keine weiteren Sicherheitsmaßnahmen getroffen wurden (z.B. Dokumentenverschlüsselung), dann kann ein solcher Datenträger unter Umständen in die falschen Hände geraten und zu einer Verletzung der Vertraulichkeit der Patientendaten führen.

Die beschriebenen Problembereiche lassen sich so zusammenfassen:

- gleichzeitige Ausführung von Anwendungen für unterschiedliche Aufgaben auf demselben Rechner;
- Verbindung der Praxis-IT mit sowohl gesicherten als auch ungesicherten externen Netzwerken;
- Speicherung und Weitergabe von patientenbezogenen Daten auf unverschlüsselten Medien.

Generelle Lösungsansätze

Im folgenden werden einige generelle Lösungsansätze sowie deren Chancen und Risiken diskutiert.

Verschlüsselung

Die Verschlüsselung von Daten ist in vielen Fällen hilfreich, jedoch nicht die alleinige Lösung. Zunächst einmal schützt Verschlüsselung im allgemeinen nur die Vertraulichkeit (nicht die Integrität) der Daten. Zur Erkennung von Integritätsverletzungen müssen andere kryptographische Verfahren hinzugezogen werden (z.B. Digitale Signatur).

Verschlüsselung kann sowohl beim Speichern von Daten auf Medien als auch beim Transport über Netzwerke eingesetzt werden. Letzteres geschieht bereits im obigen Grundmodell durch die VPN-Box. Die Verschlüsselung beim Speichern auf Medien kann in zwei Formen geschehen: durch individuelle Dateiverschlüsselung oder durch eine vollständige Medienverschlüsselung. Letzteres kann durch eine Software-Lösung, die auf dem Arzt-PC läuft, durchgesetzt werden oder automatisch durch die Medien-Hardware selbst geschehen (sogenannte Self-Encrypting Disks). Die selbstverschlüsselnden Medien bieten hier einen guten Schutz

gegen das irrtümliche Speichern auf ungeschützte Medien. Beim Einsatz von Software-Lösungen kann es jedoch passieren, dass die Anwendung entsprechender Tools vom Benutzer vergessen oder falsch konfiguriert wird.

Entscheidend sind neben der kryptographischen Stärke und Sicherheit der eingesetzten Algorithmen letzten Endes das Management und die Verteilung der zugehörigen kryptographischen Schlüssel. Eine übliche Vorgehensweise bei der Medienverschlüsselung ist die Ableitung des Schlüssels von einem Passwort. Hiermit wird jedoch die Sicherheit auf Geheimhaltung und sichere Weitergabe des Passwortes reduziert.

Zudem gilt, dass Verschlüsselung nicht dagegen helfen kann, dass unterschiedliche Anwendungen auf ein und derselben Rechnerplattform laufen und ggf. nicht auf Daten im Klartext zugreifen dürften. Wenn einmal das Passwort (oder ein sonstiger Mechanismus) aktiviert wurde, um auf das verschlüsselte Medium zuzugreifen, können auf Standardbetriebssystemen in der Regel alle Programme des eingeloggten Benutzers darauf zugreifen. Wenn Schadsoftware auf dem Rechner vorhanden ist, kann diese den Vertraulichkeitsschutz durch Verschlüsselung umgehen und die Daten ggf. im Klartext woanders hinleiten. Das gleiche gilt für einen externen Zugriff bei Fernwartung von IT-Systemen.

Virenscanner

Der übliche Ansatz gegen Schadprogramme ist der Einsatz aktueller Antiviren-Software. Während dies sicherlich eine Vielzahl von Bedrohungen verhindern oder eindämmen kann, bleibt jedoch immer ein grundsätzliches Problem: Virenscanner laufen den Angriffen immer hinterher, denn eine Erkennung kann nur von bekannten Angriffen oder Angriffsmustern erfolgen. Völlig neuartige Angriffe können damit nicht erkannt werden, z.B. sogenannte „Zero-Day-Exploits“, die bisher unbekannte Schwachstellen von Software ausnutzen.

Virenscanner helfen nicht gegen grundsätzlich mögliche Zugriffe von Software-Programmen (z.B. im Rahmen eines Software-Updates oder Fernwartung. Ebenso wenig helfen sie gegen die irrtümliche Weiterhabe durch Speicherung auf externen Medien.

Zugriffskontrolle

Um unautorisierte Zugriffe auf Daten zu vermeiden, gibt es grundsätzlich das Mittel der Zugriffskontrolle. Die bei heutigen Standardbetriebssystemen verwendeten Mechanismen konzentrieren sich jedoch immer noch verstärkt auf die Benutzer, die auf ein IT-System zugreifen. Dies ist das richtige Mittel, um genauer zu unterscheiden, welches Personal auf welche Daten und Datentypen in einer Arztpraxis oder Krankenhaus zugreifen darf. Innerhalb eines Rechnersystems bietet es oft jedoch wenig Kontrolle gegenüber einzelnen Software-Programmen, insbesondere wenn sie alle unter einem Benutzerkonto ausgeführt werden.

Theoretisch lassen sich die verschiedenen Anwendungen in jeweils eigenen Benutzerkonten ausführen. So ließen sich feingranular Rechte definieren, z.B. dass nicht der Internet-Browser auf Patientendaten zugreifen darf, sondern nur die Abrechnungssoftware, wenn sie im Abrechnungs-Benutzerkonto ausgeführt wird. Dies würde jedoch bedeuten, dass man sich bei jedem Wechsel zu einer anderen Anwendung umloggen müsste. Praktikabel wäre diese Lösung sicher nicht, deshalb findet sie auch kaum Anwendung.

Isolation

Die Isolation von IT-Systemen oder einzelnen Software-Programmen kann helfen, Bedrohungen durch Schadsoftware oder Angriffe aus dem Netz zu begrenzen. Es gibt unterschiedliche Realisierungen, die jeweils unterschiedlich stark isolieren.

- **Physische Isolation**: Hier werden separate Systeme für jeweils unterschiedliche Aufgaben verwendet. Zum Beispiel kann es dedizierte Rechner geben, die nur die medizinischen Anwendungen ausführen, dedizierte Rechner für die Abrechnung mit den KVen und wiederum dedizierte Rechner, die ans Internet angeschlossen sind. Damit die Isolation effektiv ist, dürfen diese Rechner nicht Praxis-intern miteinander vernetzt sein. Eine solche Beispielkonfiguration findet sich auch in der KV-SafeNet Dokumentation [7]. Während diese Architektur das Sicherheitsproblem der Anwendung unterschiedlicher Programme und die Verbindung in unterschiedliche Netze lösen kann, bleibt die Praktikabilität (*Usability*) auf der Strecke. Notwendige Kommunikation (z.B. Übertragung von Patientendaten aus den medizinischen Systemen in das Abrechnungssystem) wird erschwert. Außerdem erhöht es die Kosten, da zusätzliche PC-Hardware mehrfach benötigt wird.
- **Software Isolation**: Die Bereitstellung isolierter Ausführungsumgebungen kann aber auch softwareseitig (zum Teil mit Hardware-Unterstützung durch die CPU) erfolgen. Dabei gilt es hauptsächlich zwei Typen zu unterscheiden: Application Sandboxing und Virtualisierung. Beim Sandboxing-Verfahren wird einzelnen Anwendungen vom Betriebssystem ein eingeschränkter Zugriff gewährt, der sich grundsätzlich nur auf anwendungsbezogene Daten beschränkt. So ließe sich beispielsweise einstellen, dass medizinische Programme nur auf medizinische Daten zugreifen können und Abrechnungsprogramme nur auf administrative Daten. Während Sandboxing verstärkt gerade in Mobilplattformen (Android, iOS) eingesetzt wird, lässt sich langsam auch das Einfließen in Desktop-Betriebssysteme beobachten (z.B. bei MAC OS X, Chrome OS, Ubuntu Linux). Hier ist allerdings fraglich, inwiefern diese Systeme in Arztpraxen eingesetzt werden. Zudem müssen bestehende Anwendungen ggf. an das Sandboxing angepasst werden, da sie sonst von einem Vollzugriff auf das System ausgehen und bei Sandboxing sonst zu Fehlern führen. Virtualisierung bietet hier eine bessere Kompatibilität zu vorhandenen Systemen, da ein ganzes Betriebssystem (samt Anwendungssoftware) in einer virtuellen Maschine (VM) ausgeführt wird. Auf diese Weise lassen sich mehrere VMs auf einer Hardware-Plattform ausführen, die ggf. jeweils unterschiedliche Aufgaben erfüllen. Ebenso kann der Netzwerkzugriff für jede VM separat geregelt werden. Virtualisierung an sich schützt jedoch nicht davor, dass Daten irrtümlich weitergegeben oder weggespeichert werden. Sie bietet jedoch eine kostengünstigere Alternative als die physische Isolation. Die Effektivität der Isolation (d.h. deren Robustheit) hängt jedoch von der eingesetzten Virtualisierungstechnologie ab. Hier gilt es entsprechende Produkte zu prüfen (z.B. mit entsprechenden Evaluierungen nach Common Criteria).

Ganzheitliche Lösungen notwendig

Der Einsatz einer einzelnen Maßnahme ist oft nicht ausreichend, um einen ganzheitlichen Schutz der Daten im IT-System der Arztpraxis zu gewährleisten. Hier sind ganzheitliche Lösungen erforderlich, die wie in großen IT-Infrastrukturen von Krankenhäusern

oder auch Unternehmen in einer Sicherheitsarchitektur zusammengefasst werden. Lösungen, die Kompatibilität zu vorhandenen Anwendungen und IT-Systemen bieten, dürften die größten Chancen haben, akzeptiert zu werden, da sie bereits getätigte Investitionen (in IT und ggf. Schulung der Mitarbeiter) weiter nutzbar lassen.

Neben der Kompatibilität spielt die Usability, d.h. Benutzbarkeit und Benutzerfreundlichkeit, eine erhebliche Rolle. Gegebene Arbeitsabläufe sollten nicht oder nur minimal gestört werden. Insbesondere eine einfache und fehlervermeidende Administration der eingesetzten Maßnahmen ist hier enorm wichtig.

Lösungsansatz am Beispiel von MediTrust

Im Projekt MediTrust [11], das vom Land NRW und der EU teilgefördert wird, entwickelt die Forschungsgruppe Systemsicherheit der Ruhr-Universität Bochum zusammen mit der Sirrix AG eine Sicherheitsarchitektur, die die Sicherheit von Primärsystemen in Arztpraxen zum Ziel hat. Grundidee ist die Überlegung, dass es eben verschiedene Anwendungen auf derselben Hardwareplattform gibt, diese aber unterschiedlichen Sicherheitsdomänen zuzuordnen sind (z.B. Abrechnungssoftware vs. Internet-Anwendungen). Für jede dieser Domänen gibt es isolierte Ausführungsumgebungen in Form von Virtuellen Maschinen (VM), so dass Rückwärtskompatibilität von vorhandenen Anwendungen und Betriebssystemen gegeben ist. Unter diesen Ausführungsumgebungen gewährleistet ein Sicherheitskern die Isolation und die Kontrolle über den Informationsfluss: Alle Daten, die zu einer Domäne gehören, sind auch nur in Ausführungsumgebungen derselben Domäne zugreifbar. Dies wird durch Verschlüsselung des Datentransfers realisiert, sowohl über Netzwerkverbindungen als auch, wenn Daten auf externe Medien (z.B. USB-Sticks) gespeichert werden. Das zugrundeliegende Sicherheitsmodell basiert auf sogenannten „Trusted Virtual Domains“ [10]. **Abb.** 2 zeigt die Architektur.

Daten aus einer Domäne werden automatisch so verschlüsselt, dass sie nur wieder von einer Plattform gelesen werden können, die ebenfalls Ausführungsumgebungen dieser Domäne bereitstellt. Ein versehentliches Vergessen der Verschlüsselung von Speichermedien kann so verhindert werden. Gleichzeitig sorgt der Sicherheitskern dafür, dass die zugehörigen Schlüssel nur an Plattformen gegeben werden, die ebenfalls einen entsprechenden Sicherheitskern ausführen.

Der Sicherheitskern baut auf modernen CPU-Architekturen auf, die Virtualisierungsfunktionen bereitstellen und zusätzlich von einem Hardware-Sicherheitsmodul unterstützt werden, z.B. durch ein Trusted Platform Module (TPM). Dadurch lassen sich Funktionen realisieren, die beim Starten des Systems die Integrität der Softwarekomponenten überprüfbar machen und bestimmte Daten kryptographisch an diese Integritätswerte (und damit an den Sicherheitskern) binden. So können VPN-Zertifikate und Schlüsselmaterial ähnlich geschützt gespeichert werden, wie in einer VPN-Box mit Hardware-Sicherheitsmodul. Hier jedoch übernimmt der Sicherheitskern (in Zusammenarbeit mit dem TPM) die Aufgabe der VPN-Box aus dem zu Anfangs beschriebenen Grundmodell. Abb. 2 zeigt beispielsweise, dass es einmal ein virtuelles privates Netzwerk zu den eHealth-Diensten gibt und ein davon getrenntes virtuelles Netzwerk zu Internet-Anwendungen. Der Vorteil dieser Architektur ist, dass Anwendungen, die jeweils zu einem dieser Netzwerke gehören, auch nur innerhalb der zugeordneten Sicherheitsdomäne ausgeführt werden. So sind die eHealth-Anwendungen in der Beispielarchitektur zwar auf derselben Hardware-Plattform wie die Internet-Anwendungen (d.h. auf demselben Arzt-PC), aber sie werden in isolierten Bereichen ausgeführt. Eine Kommunikation zwischen diesen Domänen wird standardmäßig strikt unterbunden. Das entspricht in etwa dem Szenario, wo physisch getrennte Systeme für die jeweils unterschiedlichen Aufgaben eingesetzt werden.

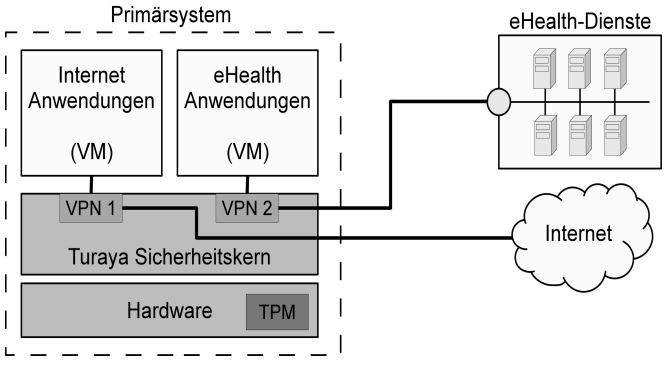

Abb. 2: Beispielarchitektur von MediTrust

Ein weiterer Vorteil ergibt sich für die Fernwartung oder Software-Updates von Anwendungen. Hier kann prinzipiell dem Software-Hersteller Zugriff auf die Anwendungen in der abgeschotteten Domäne gegeben werden, ohne dass dieser auf die Daten der anderen Domänen zugreifen kann. Zudem kann es auch den Support und die Distribution völlig vereinfachen: Software-Hersteller könnten vollständige Konfigurationen der Anwendungen samt Betriebssystem in einem Virtuell Maschinen Abbild (VM Image) bereitstellen. Dies löst Betriebssystemversionskonflikte oder Probleme durch Konfigurationen anderer Anwendungen. Denn prinzipiell jede Anwendung kann in ihrer eigenen VM-Umgebung ausgeführt werden.

Ein besonderer Augenmerk bei MediTrust liegt auf der Praktikabilität (Usability) der Lösung. Hier wird aktuell in einer umfangreichen Benutzerstudie geforscht, um Ergebnisse direkt in die Produktentwicklung einfließen zu lassen. Ein wesentlicher Aspekt hierbei ist die optimale Darstellung und die Verständlichkeit des Sicherheitskonzeptes in der graphischen Oberfläche. Während das System technisch davor schützen kann, dass sensitive Daten nicht in die falsche Domäne gelangen, kann ein Mensch immer noch einen Fehler bei der Dateneingabe machen, z.B. Patientendaten aus Versehen in eine Internet-Anwendung eingeben statt in die Abrechnungssoftware. Den Anwendern muss also unmissverständlich klar sein, mit welcher Anwendung (in welcher Domäne) sie gerade arbeiten.

Ein weiterer Aspekt der Usability ist die Integration der Architektur in die Praxis-IT, ohne vorhandene Arbeitsabläufe zu beeinträchtigen. Hierzu müssen die Domänen der unterschiedlichen Anwendungen optimal definiert werden, so dass Einfachheit der Arbeitsabläufe und Datensicherheitsziele gleichermaßen erfüllt werden. Dies ist oft keine triviale Aufgabe.

Schließlich bleibt noch zu sagen, dass die Isolation der Domänen nicht dagegen helfen kann, wenn die in der Domäne ausgeführte Anwendung selbst ein Schadprogramm ist. Die Isolation kann nur den dadurch eventuell entstehenden Schaden auf die Domäne bezogen eindämmen. Weitere organisatorische Maßnahmen sind notwendig, wie z.B.

Zertifizierungen und Evaluierungen der eingesetzten Anwendungen. Der Sicherheitskern kann allerdings die technische Durchsetzung unterstützen, dass nur zertifizierte Anwendungen in bestimmten Domänen ausgeführt werden.

Fazit

Bei eHealth-Architekturen wird oftmals davon ausgegangen, dass die Primärsysteme in den Arztpraxen vollkommen vertrauenswürdig sind. Wenn man diese Annahme negiert, zeigen sich jedoch zahlreiche Aspekte, die bisher nicht zufriedenstellend gelöst sind. Es gibt eine Reihe genereller Ansätze, doch letztendlich müssen ganzheitliche Lösungen her. Eine mögliche Option wurde anhand des prototypischen Projektes „MediTrust“ aufgezeigt.

Literatur

[1] Gesellschaft für Telematikanwendungen der Gesundheitskarte (gematik), http://www.gematik.de

[2] Projektinitiative Elektronische Fallakte (EFA), http://www.fallakte.de/

[3] Kassenärztliche Bundesvereinigung: „KV-SafeNet: Bundesweit vernetzt mit dem Rundum-sorglos-Paket“, http://www.kbv.de/24874.html

[4] Bundesamt für Sicherheit in der Informationstechnik: „Common Criteria Schutzprofil (Protection Profile) für einen Konnektor im elektronischen Gesundheitswesen, Schutzprofil 1: Anforderungen an den Netzkonnektor (NK-PP)“, BSI-CC-PP-0033, 2007.

[5] Kassenärztliche Bundesvereinigung: „Richtlinie KV-SafeNet“, Version 3.1, Oktober 2011.

[6] Kassenärztliche Bundesvereinigung: „Merkblatt KV-SafeNet-Router“, Version 1.0, Oktober 2011.

[7] Kassenärztliche Bundesvereinigung: „Merkblatt Sicherheitsanforderungen KV-SafeNet-Arbeitsplätze“, Version 1.1, Oktober 2011.

[8] L. Palm: „Praxisüberwachung“, Die Datenschleuder #95, 2011.

[9] Michael Meyer, Ulf Hönick: „Sichere Telematikinfrastruktur im Gesundheitswesen“, Datenschutz und Datensicherheit (DuD) 3/2006, S.155 ff.

[10] L. Catuogno, H. Löhr, M. Manulis, A.-R. Sadeghi, C. Stüble, M. Winandy: „Trusted Virtual Domains: Color Your Network“, Datenschutz und Datensicherheit (DuD) 5/2010, S.289 ff.

[11] RUBTrust/MediTrust Homepage: http://www.rubtrust-meditrust.de