Grundzüge eines Sicherheitskonzepts für Arztpraxen mit Hilfe von Attack Trees und unter Berücksichtigung der Gesundheitstelematik

Raffael Rittmeier, Dr. Karsten Sohr

Fachbereich Mathematik und Informatik
Universität Bremen
Bibliothekstr. 1
28359 Bremen
raffael@informatik.uni-bremen.de
sohr@tzi.de

Abstract: Ziel dieser Arbeit ist es, den Schutz sensibler Patientendaten zu verbessern. Es wird eine Vorgehensweise zur Erstellung eines Sicherheitskonzepts für Arztpraxen skizziert. Dabei werden die entsprechenden Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI) durch Bedrohungsbäume (*attack trees*) erweitert. Damit können z. B. Bedrohungen analysiert werden, die durch die Einführung neuer Technologien entstehen können. Ein spezieller IT-Grundschutzbaustein für Arztpraxen und eine freiwillige Zertifizierung werden diskutiert.

1 Einleitung

Arztpraxen setzen heute zunehmend auf digitalisierte Arbeitsprozesse. So sind Ärzte ab 2010/11 verpflichtet ihre Abrechnung leitungsgebunden elektronisch zu übertragen, statt wie bisher quartalsweise einen Datenträger bei der Kassenärztlichen Vereinigung einzureichen [KBV08]. Mit der neuen elektronischen Gesundheitskarte (eGK) sollen die Beteiligten des Gesundheitswesens über das Internet vernetzt werden. Unter Protest der Ärzteschaft macht die aktuelle Gesetzgebung die Onlineanbindung für Arztpraxen verpflichtend [AEZ10]. Durch die zunehmende Digitalisierung und Vernetzung wird die Informationssicherheit in Arztpraxen zunehmend wichtiger.

Ärzte speichern und verarbeiten medizinische Daten ihrer Patienten und damit nach Bundesdatenschutzgesetz (BDSG) besonders schützenswerte personenbezogene Informationen. Diese Daten müssen unter allen Umständen vertraulich behandelt werden. Bei der elektronischen Speicherung und Verarbeitung von Patientendaten müssen auch die Computersysteme besonders geschützt sein, um unbefugten Zugriff zu verhindern. Durch die Verpflichtung zur Online-Verbindung entstehen jedoch zusätzliche Risiken, z. B. durch Fremdzugriff.

2 Ziele

Am Beispiel von Arztpraxen wird in diesem Beitrag eine Vorgehensweise vorgestellt, um die Informationssicherheit im Gesundheitswesen zu untersuchen und zu verbessern. Bedrohungen und Risiken werden erfasst und analysiert. Anschließend werden Maßnahmen zur Behandlung der Risiken vorgeschlagen. Daraus ergeben sich die Grundzüge eines Sicherheitskonzepts für Arztpraxen, bei dem der Schutz von Patientendaten und deren Vertraulichkeit im Vordergrund stehen.

Die am IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) ausgerichtete Vorgehensweise wird durch Bedrohungsbäume *(attack trees*) erweitert. Diese Darstellung ermöglicht es, die Ärzte und ihre Angestellten besser für den Datenschutz und die Informationssicherheit der Patientendaten zu sensibilisieren.

3 Methoden

Grundlage für diesen Beitrag ist die Untersuchung von drei Bremer Arztpraxen, in denen jeweils bis zu 400 Patienten pro Tag behandelt werden und die ihre Dokumentation weitgehend elektronisch führen [Ri09]. In Gesprächen mit den für die EDV verantwortlichen Ärzten wurden die Geschäftsprozesse und die Infrastruktur der Arztpraxen erfasst. Die Daten wurden durch die Infrastrukturanalyse und die Schutzbedarfsermittlung nach dem IT-Grundschutz des BSI aufbereitet [BSI08a]. Die vom BSI empfohlene Vorgehensweise zur Erstellung einer Bedrohungs- und Risikoanalyse wurde durch Bedrohungsbäume erweitert [BSI08b]. In der erweiterten Risikoanalyse wurden die relevanten Bedrohungen bewertet [Ec09]. Anschließend wurde ein Maßnahmenkatalog zusammengestellt, um die Risiken zu mindern.

Bezüglich der Einführung der Telematikinfrastruktur (TI) wurden u.a. mögliche Bedrohungen ermittelt, die durch die Integration des Konnektors in das Praxisnetz entstehen können. Als Quellen dienten v. a. die Spezifikationen der gematik.

3.1 Verwendung von Bedrohungsbäumen

Bruce Schneier hat die Bedrohungsbäume im Bereich der IT-Sicherheit 1999 eingeführt [Sc99]. Diese sind von der Fehlerbaumanalyse (*fault tree analysis*) aus dem „Safety“-Bereich abgeleitet. Dort werden Baumstrukturen z. B. im Rahmen von Sicherheitsüberprüfungen kerntechnischer Anlagen eingesetzt [Ha81].

Bedrohungsbäume zeigen Abhängigkeiten zwischen verschiedenen Ereignissen bzw. Angriffsschritten auf. Gängig sind die grafische Darstellung sowie die Textform. In dieser Arbeit wird Letztere gewählt, da sie für detaillierte Bäume übersichtlicher ist [Sc04].

Ein Baum besteht aus einer Menge von Knoten. Ein Knoten kann dargestellt werden als:

- Menge von Knoten, die alle erfüllt werden müssen, damit ein Angriff erfolgreich ist. In diesem Fall spricht man von einer UND-Verknüpfung.
- Menge von Knoten, von denen mindestens ein Knoten erfüllt werden muss, damit der Angriff erfolgreich ist. In diesem Fall spricht man von einer ODER-Verknüpfung.
- Knoten, dem keine weiteren Knoten mehr folgen (Blätter).

Das Angriffsziel befindet sich im obersten Knoten, der sogenannten Wurzel.

3.2 Beispiele

Im Folgenden werden zwei Beispiele für Bedrohungsbäume angegeben. Diese behandeln Angriffe auf ein Praxisverwaltungssystem (PVS).

Beispiel 1:

Angriffsziel: Unbefugter Zugriff auf vertrauliche Patientendaten im PVS

1 Inbesitznahme von Patientendaten, die auf dem PVS-Server gespeichert sind (ODER)

1.1 Physikalischer Angriff auf den PVS-Server (UND)

1.1.1 Zutritt zur Praxis (ODER)

1.1.1.1 Zutritt während der Sprechzeiten

1.1.1.2 Zutritt außerhalb der Sprechzeiten

1.1.2 Zutritt zum Serverraum

1.1.3 Zugriff auf PVS-Server und gespeicherte Patientendaten

1.2 Entfernter Angriff auf den PVS-Server

Erfolgreiche Angriffsszenarien von Beispiel 1 sind demnach: {1.1.1.1, 1.1.2, 1.1.3}, {1.1.1.2, 1.1.2, 1.1.3}, {1.2}.

Der Vorteil von Bedrohungsbäumen ist, dass sie wiederverwendbar sind und Teilbäume unabhängig voneinander betrachtet werden können. In Beispiel 2 wird der entfernte Angriff auf den PVS-Server (Subziel 1.2) genauer analysiert.

Beispiel 2:

Subziel 1.2: Entfernter Angriff auf den PVS-Server (ODER)

1.2.1 Anschluss eines eigenen Systems in der Praxis (UND)

1.2.1.1. Physikalischer Anschluss an das Praxisnetz

1.2.1.2. Gültige Netzkonfiguration einstellen

1.2.1.3. IP-Adresse des PVS-Servers beschaffen

1.2.1.4. Erfolgreicher Angriff auf Betriebssystem oder PVS-Software und Auslesen von Patientendaten

1.2.1.5. {1.1.1}

1.2.2 Lokale Übernahme eines PVS-Clients (UND)

1.2.2.1. Überwinden der Betriebssystem-Authentifizierung

1.2.2.2. Überwinden der PVS-Authentifizierung und Einsehen bzw. Export von Patientendaten

1.2.2.3. {1.1.1}

1.2.3 Entfernter Angriff über ISDN

1.2.4 Entfernter Angriff über DSL

Um erfolgreich zu sein, benötigen die Angriffsschritte 1.2.1 und 1.2.2 die Erfüllung des bereits aufgeführten Angriffsschritts 1.1.1. Um Redundanz zu vermeiden, wird lediglich auf den entsprechenden Teilbaum verwiesen. Unter Beibehaltung der Übersichtlichkeit können die Angriffsziele so bis zur gewünschten Tiefe verfeinert werden. Anschließend werden die Bedrohungen bewertet und Maßnahmen vorgeschlagen.

4 Ergebnisse

Die bekannten Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit gelten auch für den Schutz der Patientendaten. Schwerpunkt dieser Arbeit war die Sicherstellung der Vertraulichkeit der Daten. Das PVS verarbeitet die sensiblen Daten, die zusätzlich in Archiven und auf externen Speichermedien gesichert werden. Eine physikalische Trennung zwischen Internet und PVS minimiert die Risiken eines Internetanschlusses. Ist die strikte Trennung nicht möglich, müssen organisatorische und technische Schutzmaßnahmen die Vertraulichkeit der Patientendaten sicherstellen, z. B. durch verhaltensregelnde Richtlinien und den Einsatz von Firewalls und Intrusion Detection Systems (IDS). Weitere Bedrohungen entstehen z. B. durch Diebstahl oder Verlust von Speichermedien. Starke Verschlüsselungsmechanismen stehen dem entgegen.

Die geplante Telematikinfrastruktur soll die Akteure des Gesundheitswesens miteinander vernetzen. Verschiedene Telematikanwendungen werden ihre Daten in einem vernetzten System speichern. Der Versichertenstammdatendienst (VSDD) verarbeitet z. B. die verwaltungsrelevanten Daten der Patienten. Später sollen der elektronische Arztbrief und die elektronische Patientenakte (ePA) folgen.

Für Arztpraxen ist der Konnektor ein entscheidender Bestandteil. Er soll das Praxisnetz sicher mit der Telematikinfrastruktur verbinden und vor Bedrohungen aus dem Internet schützen. Werden die ausführlichen Vorgaben aus Spezifikationen und Common Criteria-Schutzprofil (*protection profile*) bei der Implementierung befolgt, wird die Vertraulichkeit der Patientendaten bei der Datenverbindung gewährleistet [BSI07]. Die Technologie ist jedoch komplex und eine fehlerfreie Implementierung kann nicht garantiert werden. Hinzu kommt, dass der korrekte Einsatz in der Arztpraxis gewährleistet werden muss. Durch die zusätzliche Technik erhöht sich der administrative Aufwand. Ohne einen IT-Dienstleister werden die Inbetriebnahme und die Wartung Probleme für die Arztpraxen darstellen. Verbesserungsbedarf besteht ebenfalls bei der Anbindung der PVS. Eine verschlüsselte Übertragung soll zwar ermöglicht werden, ist jedoch nicht vorgeschrieben [Ge08]. Die Technologie der Telematikinfrastruktur mag zwar einen entsprechenden Sicherheitsstandard aufweisen; sie gilt jedoch nicht zwingend für die Systeme beim Leistungserbringer wie z. B. bei dem PVS oder dem Praxisnetz.

Eine weitere Bedrohung ergibt sich durch die gesetzlich vorgesehene Datenwiederherstellung. Bei Verlust der elektronischen Gesundheitskarte oder beim Wechsel der Verschlüsselungsstärke soll der geheime Schlüssel automatisch rekonstruiert werden, um die sensiblen Patientendaten für eine neue Karte zu verschlüsseln. Die Sicherheit asymmetrischer Verschlüsselung basiert jedoch auf der Geheimhaltung des privaten Schlüssels. Wenn dieser durch Dritte rekonstruiert werden kann, ergibt sich ein entsprechendes Sicherheitsproblem.

5 Diskussion

Gesetzliche Vorgaben und die Einführung von Telematiksystemen fordern einen Internetanschluss der Arztpraxen. Dabei muss der unbefugte Zugriff auf Patientendaten unbedingt unterbunden werden. Ein spezieller IT-Grundschutzbaustein des BSI wäre sinnvoll, denn die bestehenden Empfehlungen genügen nicht und werden in der Praxis nur selten beachtet. Maßnahmen zur Verbesserung der Informationssicherheit müssen geeignet sein, um die optimierten Abläufe in den Arztpraxen nicht zu behindern. Des Weiteren müssen die Maßnahmen konkret genug sein, damit sie umgesetzt und überprüft werden können. Hier bieten sich Grundschutzbausteine an, gegen die bei einer Zertifizierung evaluiert werden könnte. Basierend auf der Evaluierung könnte dann auch durch die Bundesärztekammer bzw. Kassenärztliche Bundesvereinigung ein Siegel für Informationssicherheit und Datenschutz vergeben werden. Eine Zertifizierung wird sicherlich nur auf freiwilliger Basis möglich sein.

Attack Trees ergänzen die Bedrohungs- und Risikoanalyse sinnvoll. Risiken können übersichtlich dargestellt werden und die Sensibilisierung für Sicherheitsprobleme wird erleichtert. Der Aufwand lässt sich reduzieren, da die Baumstruktur das Wiederverwenden einzelner Teilbäume ermöglicht.

Organisatorische Maßnahmen, wie z. B. Schulungen, dürfen nicht vernachlässigt werden. Die Einhaltung des BDSG in seiner aktuellen Fassung muss stärker überprüft werden. Dazu gehören nach § 42a BDSG auch die konsequente Meldung von Datenlecks und die Benachrichtigung der von Datenverlusten Betroffenen.

Die Einführung der elektronischen Gesundheitskarte ist eine Möglichkeit, Patientendaten besser zu schützen. Es wird jedoch nicht ausreichen, wenn die neuen Telematiksysteme sicher konzipiert werden. Die bestehenden Infrastrukturen in den Arztpraxen müssen ebenso kritisch untersucht und dürfen nicht weiter ignoriert werden. Es wäre wünschenswert, wenn die Betreibergesellschaft klare Sicherheitsvorgaben für die PVS veröffentlichen würde. Da die gematik dies nicht als ihren Aufgabenbereich versteht, sind die zuständigen Ärztekammern, Kassenärztlichen Vereinigungen und Datenschutzaufsichtsbehörden in der Pflicht, Mechanismen zu entwerfen, um die Sicherheit der sensiblen Daten im Gesundheitswesen zu verbessern. Die in diesem Beitrag vorgestellte Vorgehensweise könnte als Basis genutzt werden, um ein Auditverfahren speziell für Arztpraxen zu entwickeln. So könnten der Datenschutz und die Informationssicherheit im Gesundheitswesen verbessert werden.

Literaturverzeichnis

[AEZ10] Online-Stammdatenabgleich kommt jetzt ins Gesetz. In: Ärzte Zeitung online, 2010, http://www.aerztezeitung.de/praxis_wirtschaft/gesundheitskarte/article/607574/online-stammdatenabgleich-kommt-jetzt-gesetz.html (Abruf am 09.08.10).

[BSI07] Bundesamt für Sicherheit in der Informationstechnik: Common Criteria Schutzprofil (Protection Profile) für einen Konnektor im elektronischen Gesundheitswesen. Bonn, 2007, https://www.bsi.bund.de/cae/servlet/contentblob/480298/publicationFile/29312/PP0033b_pdf.pdf (Abruf am 09.08.2010).

[BSI08a] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise. Bonn, 2008, https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30758/standard_1002.pdf (Abruf am 09.08.2010).

[BSI08b] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz. Bonn, 2008, https://www.bsi.bund.de/cae/servlet/contentblob/471454/publicationFile/30757/standard_1003.pdf (Abruf am 09.08.10).

[Ge08] Gematik: Konnektorspezifikation 2.10.0. Berlin, 2008, http://www.gematik.de/cms/media/dokumente/release_2_3_4/release_2_3_4_dezkomponenten/gematik_KON_Konnektor_Spezifikation_V2100.pdf (Abruf am 09.08.2010), S. 136.

[Ec09] Eckert, C.: IT-Sicherheit: Konzepte-Verfahren-Protokolle. 6. Auflage, Oldenbourg Wissenschaftsverlag, München, 2009.

[Ha81] Haasl, D.F., et. al.: Fault tree handbook. Office of Nuclear Regulatory Research, Nuclear Regulatory Commission, Washington, DC (USA). 1981 (NUREG-0492). – Technical Report.

[KBV08] Kassenärztliche Bundesvereinigung: Änderungen der Richtlinien für den Einsatz von IT-Systemen in der Arztpraxis. In: Dtsch Arztebl, 105, 2008, Nr. 12, S. A–650 / B–570 / C–558.

[Ri09] Rittmeier, R.: Grundzüge eines Sicherheitskonzepts für Arztpraxen unter Berücksichtigung der Gesundheitstelematik. Diplomarbeit, Universität Bremen, 2009.

[Sc99] Schneier, B.: Attack Trees. In: Dr. Dobb's Journal, 24, 1999, Nr. 12, S. 21–29.

[Sc04] Schneier, B.: Secrets and lies: digital security in a networked world. Wiley, Indianapolis, Ind., USA, 2004, S. 324.