Please quote as: Sunyaev, A.; Mauro, C.; Huber, M. & Leimeister, J. M. (2008): Bewertung und Klassifikation von Bedrohungen im Umfeld der elektronischen Gesundheitskarte. München

Bewertung und Klassifikation von Bedrohungen im Umfeld der elektronischen Gesundheitskarte

Ali Sunyaev, Michael J. Huber, Christian Mauro, Jan Marco Leimeister, Helmut Krcmar

Lehrstuhl für Wirtschaftsinformatik
Technische Universität München
Boltzmannstraße 3
85748 Garching bei München
{sunyaev, hubermic, mauro, leimeister, krcmar}@in.tum.de

Abstract: Dieser Beitrag identifiziert und klassifiziert mögliche Angreifer und Angriffe rund um die Einführung der neuen elektronischen Gesundheitskarte bzw. rund um die Telematik-Infrastruktur in Deutschland aus sicherheitstechnischer Perspektive. Dadurch soll mehr Transparenz zur IT-Sicherheit für Patienten und Leistungserbringer geschaffen und mögliche Sicherheitslücken identifiziert werden, um projekt-begleitende Lösungen rechtzeitig vor der flächendeckenden Einführung der elektronischen Gesundheitskarte erarbeiten zu können. Die vorgeschlagene Klassifikation der Bedrohungen wird in der Test- und Modellregion Ingolstadt als Teil der begleitenden Sicherheitsevaluation angewendet.

1 Einführung

Die Einführung der elektronischen Gesundheitskarte (eGK) erfolgt, aufgrund der Komplexität und des Umfanges des weltweit größten Telematik-Projektes, in mehreren Schritten. Nach den gesetzlich vorgeschriebenen Labortests wird die Einführung der elektronischen Gesundheitskarte in ausgewählten Testregionen erprobt. Anschließend soll die eGK schrittweise flächendeckend eingeführt werden. Die Umsetzung dieser gesetzlichen Vorgaben findet in Bayern in der Test- und Modellregion Ingolstadt statt. Die in dieser Testregion zu realisierenden Sicherheitsmaßnahmen (z.B. die zentrale Verwaltung von Gesundheitskarten im stationären Umfeld [Ma07]) werden nun durch eine Sicherheitsevaluation im Rahmen des Projektes „HatSec“[1] überprüft. Dadurch soll mehr Transparenz für die Anwender geschaffen werden. Weiterhin sollen sicherheitstechnische Fragen und Unsicherheiten von Seiten der Nutzer (sowohl Patienten als auch Leistungserbringer) überwunden werden.

Die Bewertung und Klassifikation der möglichen Bedrohungen ist ein Bestandteil der anstehenden Sicherheitsevaluation [Su07] in der Testregion. Dadurch können rechtzeitig vor der flächendeckenden Einführung der eGK wissenschaftlich abgeschätzte und evtl. gegebene Angreifer- und Angriffsarten transparent nach außen kommuniziert werden. Außerdem würde eine Klassifikation und Bewertung der Angreifer- und Angriffsarten zur Identifizierung von möglichen Sicherheitslücken rund um die eGK-Einführung in den Testregionen und deren problemspezifischen Lösungsvorschlägen beitragen.

[1] Health Care Telematics Security, http://www.ehealth-tum.de/hatsec

2 Identifizierung und Klassifikation der Angreifer

Um die Sicherheit eines Systems differenziert bewerten zu können, ist es nötig, mögliche Angreifer zu kennen und zu bewerten. So können einige Angreifer z.B. über ein beachtliches Wissen und ausgeprägte Fähigkeiten im Bereich der Informationstechnologie verfügen, andere hingegen über viel Kapital, mit dem sich Wissen und spezialisierte Technik finanzieren lassen. [Ge04] propagiert das in Abbildung 1 skizzierte Modell, das die Angreifer nach den Kriterien Know-how, Ressourcen- und Zeiteinsatz klassifiziert.

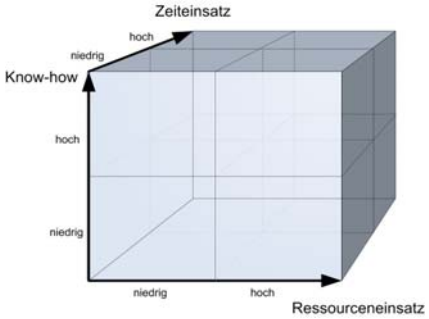

Abbildung 1: Angreifermodelle (Quelle: In Anlehnung an [Ge04])

Bezüglich der Ziele, die von den jeweiligen Angreifergruppen verfolgt werden, nennt Schneier „[…] Schaden, finanziellen Gewinn, Information, usw." [Sc00], [Ge04] zusätzlich noch Wettbewerbsvorteil und Machtinteresse. Diese Ziele werden in der folgenden Klassifizierung als Basisziele der Angreifer verwendet und um weitere, typische Ziele erweitert. Eine Einschätzung der Relevanz der Angreifergruppe im Umfeld der eGK erfolgt plausibilitätsbasiert und ist in Tab. 1 nach den bereits definierten Kriterien subjektiv bewertet und zusammengefasst.

Angreifer-Gruppe	**Ziele**	**Know-How**	**max Res.**	**max Zeit**
Hacker	Wissensgier, Interesse am System, Publicity / Selbstdarstellung / Ansehen / Ruhm, Eigene Weiterbildung, „Ehrbare Ziele", Vandalismus, (Auftrags-) Diebstahl von Informationen.	70-100	5	80
Skript Kiddies	Vandalismus, Neugierde, Publicity / Selbstdarstellung / Ansehen / Ruhm, Antrieb aus Langeweile / Spieltrieb.	0-30	1	20
Industrie-spionage	Wettbewerbsvorteil, Geschäftsschädigung der Konkurrenz.	0-100	60	70
Böswillige Insider	Rache, Finanzielle Interessen und Vorteile, Publicity, Informationsdiebstahl bei Firmenwechsel.	50-100	5	60
Organisiertes Verbrechen	Finanzielle Interessen, Schaffung von Informationen, Beschaffung von Gütern.	0-100	100	100
Malware	Vandalismus, Selbstverbreitung, Informationsdiebstahl, Publicity / Selbstdarstellung / Ansehen / Ruhm des Entwicklers	50-100	-	100
(Cyber-) Terrorismus	Zerstörung der Infrastruktur, Blockade der Infrastruktur, Verbreitung von Angst und Schrecken	0-100	30	90
Medien	Publicity, Medianwirksames Aufdecken von Schwachstellen	50-100	10	40
Die Einschätzungen zu „Know-How", „Ressourceneinsatz" und „Zeiteinsatz" wurden jeweils in einer Skala von 0 bis 100 vorgenommen, wobei 0 für den minimalen und 100 für den maximalen Wert stehen.				

Tabelle 1: Klassifikation der Angreifergruppen im Umfeld der eGK (Quelle: Eigene Darstellung)

Hacker (vgl. [Sc00], [Ge04] und [Ec06]): Im Bereich der eGK wird in der Anfangsphase vermutlich mit einem großen Interesse seitens der Hacker zu rechnen sein, was vor allem aus der Größe des Telematik Projekts und der Brisanz der betreffenden Daten folgt. Nach der anfänglichen Interessenswelle wird der eigenen Einschätzung nach hauptsächlich mit wenigen, hoch spezialisierten Angriffen aus dieser Gruppe zu rechnen sein (möglicherweise auch im Auftrag Dritter).

Skript Kiddies (vgl. [Sc00], [Ge04] und [Ec06]): Durch die große Anzahl von Skript Kiddies ist voraussichtlich vermehrt im Bereich derjenigen Angriffe, die kaum abgewehrt werden können (z.B. verteilte Denial-of-Service Angriffe), mit einer relativ hohen Bedrohung zu rechnen. Ebenso ist vorstellbar, dass im Bereich der Primärsysteme Probleme durch unzureichend gewartete Infrastrukturkomponenten auftreten werden.

Industriespionage (vgl. [Sc04], [Ge04] und [Ec06]): Im Bereich der eGK wäre Industrie- und Wirtschaftsspionage unter den Leistungsträgern oder Leistungserbringern denkbar, um z.B. einen Wettbewerbsvorteil gegenüber ihrer Konkurrenz zu erlangen.

Böswillige Insider (vgl. [Sc00] und [Ec06]): Böswillige Insider können in allen Bereichen des Gesundheitswesens vorkommen. Denkbar wären Insider sowohl aus zentralen Bereichen der Telematikinfrastruktur (TI) ebenso wie aus den dezentralen Bereichen, in denen sich Kostenträger und Leistungserbringer befinden.

Organisiertes Verbrechen (vgl. [Sc00], [Ge04] und [Ec06]): Das Gesundheitswesen stellt für das organisierte Verbrechen u.U. ein interessantes und lukratives Ziel dar. Denkbar ist z.B. potentieller Handel mit gefälschten Gesundheitskarten, das Erschleichen von Leistungen durch Manipulation von eGK, eRezept etc., Erpressung durch Datendiebstahl, Verkauf von gestohlenen medizinischen Profilen, usw.

Malware (vgl. [Ge04] und [Ec06]): Analog zu allen anderen IT-Systemen ist auch die eGK Infrastruktur durch Malware gefährdet. Vor allem die dezentralen Bereiche, die unter Verwaltung der Leistungserbringer stehen, sind gefährdet. In diesen Bereichen steht nicht zwingend die nötige Expertise für den Aufbau und die Erhaltung eines ausreichenden Schutzes vor Malware zur Verfügung, wie dies bei den zentral betreuten Komponenten und dem dazugehörigen IT-Fachpersonal der Fall ist.

(Cyber-) Terrorismus (vgl. [Sc00] und [Ne99]): Alle gesetzlich versicherten Patienten sind in die Prozesse der TI involviert. Die Sicherheit der TI ist unter Umständen essentiell für Leib und Leben eines Versicherten. Aus diesen Gründen ist die TI ein mögliches Ziel für Angriffe terroristischer Natur. Je weiter die TI mit dem Gesundheitssystem verwächst, bzw. je mehr das Gesundheitssystem von Verfügbarkeit und Funktionalität der TI abhängt, desto fatalere Auswirkungen hätte die Zerstörung bzw. Blockade derselben.

Medien: Vor allem in den Anfangsphasen der Einführung der eGK ist mit Angriffen seitens der Medien zu rechnen. Eine exklusive, publicity-trächtige Story, die z.B. die hohen Kosten der eGK Einführung nach der Entdeckung vermeintlicher Schwachstellen in Frage stellt, würde von Seiten der Medien auf ein beträchtliches Interesse stoßen.

Es wurde gezeigt, dass es eine Vielzahl an Angriffsgruppen mit den unterschiedlichsten

Motiven und Möglichkeiten gibt. Der nächste logische Schritt ist nun die Identifizierung möglicher Angriffsarten.

3 Identifikation und Klassifikation von Angriffsarten

Analog zur Klassifikation der Angreifer im vorangegangenen Kapitel gilt es auch die potentiellen Angriffsarten gegen die Telematikinfrastruktur nach geeigneten Kriterien zu systematisieren. Entscheidend für eine Unterscheidung der Angriffe können sowohl die Herkunft eines Angriffs, als auch dessen Intention und technische Basis sein. Im Folgenden werden Angriffe zuerst gemäß [Ec06] und [Ge04] nach ihrer technischen Basis und ihrer Herkunft differenziert, anschließend erfolgt eine Unterteilung nach ihrer Intention (vgl. [Sc00]). Die Klassifikation der Angriffe ist in Abbildung 2 zusammengefasst.

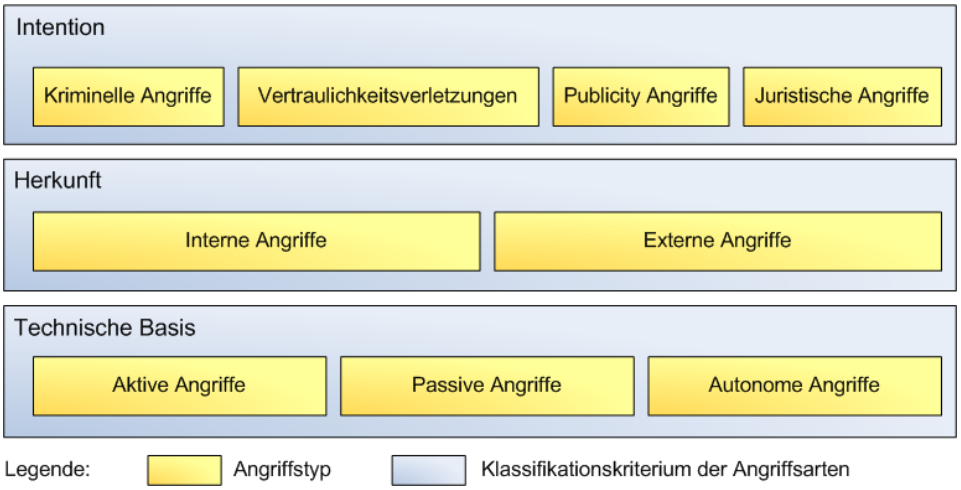

Abbildung 2: Klassifikation der Angriffe (Quelle: Eigene Darstellung)

Aktive/Passive Angriffe: Im Gegensatz zu passiven Angriffen kann ein Angreifer bei einem erfolgreichen aktiven Angriff die Daten, die auf den verteilten Servern der TI liegen, verändern. Ebenso wie das Verändern und / oder Wiedereinspielen von mitgehörten Daten, gehören zu dieser Klasse auch die Gruppen der Spoofing und Denial-of-Service Angriffe. Die eGK-Infrastruktur wird bei der Inbetriebnahme aller Voraussicht nach vor allem diesen Angriffsarten ausgesetzt sein.

Autonome Angriffe: Eine dritte Klasse der Angriffe sind autonome Angriffe. Hierzu zählen Angriffe, die von Schadsoftware (Malware) selbständig und in der Regel ohne weiteres Zutun eines Angreifers ausgeführt werden (z.B. Würmer). Wie bereits erwähnt sind insbesondere die dezentralen Bereiche der TI gefährdet.

Interne und externe Angriffe: Die Unterscheidung zwischen internen und externen Angriffen erfolgt - wie aus der Bezeichnung ersichtlich - danach, ob der Angriff von außerhalb der TI oder von innerhalb erfolgt. Im Umfeld der TI im Gesundheitswesen sind beide Varianten vorstellbar.

Kriminelle Angriffe: „Wie kann ich durch Angreifen des Systems maximalen finanziellen Gewinn erzielen?“ ist die Leitfrage aller krimineller Angriffe [Sc00]. Kriminelle Angriffe werden von denjenigen Angreifergruppen durchgeführt, die laut Klassifikation in Abschnitt 2 finanzielle Interessen zum Ziel haben. Aus datenschutzrechtlicher Sicht gebührt dieser Angriffsart ein besonderes Augenmerk. So könnten sensible medizinische Informationen zum Verkauf an Dritte freigegeben werden.

Vertraulichkeitsverletzungen: Vertraulichkeitsverletzungen können in Teilen zur Klasse der kriminellen Angriffe gezählt werden, wobei nicht alle Vertraulichkeitsverletzungen illegal sein müssen. Laut [Sc00] sind in der Klasse der Vertraulichkeitsverletzungen zwei Vorgehen zu differenzieren: Gezielte Angriffe einerseits, Data-Harvesting andererseits. Data-Harvesting bezeichnet das Vorgehen, verwertbare, oft frei verfügbare Informationen einzusammeln, anzuhäufen und daraus beispielsweise mittels Data-Mining weitere, nützliche Informationen abzuleiten. Die administrativen Patienteninformationen sind bei dieser Angriffsart das primäre Ziel. Ein dagegen legales Beispiel für Data-Harvesting ist das Payback System, bei dem Millionen von Konsumenten ihre Kaufgewohnheiten gegen kleine Prämien Marktforschungsunternehmen überlassen. Im Gegensatz dazu stehen direkte Angriffe wie z.B. Stalking oder Industriespionage. Im Bereich der Vertraulichkeitsverletzungen rund um die eGK sind die folgenden Angriffe vorstellbar: Überwachung, entsprechende Nutzung großer Datenbanken, Analyse des Datenverkehrs sowie massive elektronische Überwachung.

Publicity Angriffe: Publicity Angriffe haben das Ziel, durch den erfolgreichen Angriff eines Systems selbst Medienpräsenz zu erlangen. Interessensgruppen für diese Art von Angriff in der Domäne Gesundheitswesen sind gemäß der Klassifikation aus Kapitel 2 Hacker, Skript Kiddies, Insider, Malware und die Presse.

Juristische Angriffe: Juristische Angriffe zielen darauf ab, die (oft technisch weniger versierte) Justiz davon zu überzeugen, dass ein System eine Schwachstelle besitzt, um den Glauben an dessen vermeintliche Sicherheit in Misskredit zu bringen. Als Beispiel sei folgender Fall genannt: Die Strafverfolgungsbehörde verwendet das Mobiltelefon eines Verdächtigen, um dessen Position zu orten und ihm dadurch die Beteiligung an einer Straftat nachzuweisen. Ein juristischer Angriff wäre es nun zu beweisen, dass die Teilnehmerkennung von Mobilfunknutzern gefälscht und somit der Verdächtige durch dieses Mittel nicht 100%ig identifiziert werden kann. Das Ziel juristischer Angriffe ist es also nicht, „[…] die Schwäche in einem System auszunutzen und nicht einmal, eine Schwäche in einem System zu finden. Das Ziel ist hier, Richter und Geschworene (die wahrscheinlich nicht technisch bewandert sind) davon zu überzeugen, dass das System eine Schwäche haben könnte, das System in Misskredit zu bringen und ausreichend Zweifel beim Gericht zu erwecken, dass das System nicht perfekt ist, um die Unschuld des Mandanten zu beweisen.“ [Sc00]. Solche Angriffe sind von Seiten bzw. im Auftrag der Leistungserbringer im Gesundheitswesen vorstellbar.

4 Zusammenfassung und Ausblick

Im vorliegenden Beitrag wurden die Bedrohungen im Umfeld der elektronischen Gesundheitskarte klassifiziert und bewertet. Die Besonderheiten der Sicherheitsevaluation

der eGK liegen insbesondere in der Größe des Gesamtprojekts, der Sensibilität der Daten sowie der hohen Medienwirksamkeit. Daraus folgt zum einen, dass mit einer großen Anzahl an Angreifern mit verschiedensten Motiven und Mitteln zu rechnen ist, und zum anderen, dass durch die Komplexität des Projektes (insbesondere durch die hohe Anzahl beteiligter Systeme) die Wahrung der Sicherheit entsprechend vielschichtig ist. Die möglichen Sicherheitsprobleme werden gemäß der durchgeführten Klassifikation und Bewertung der Bedrohungen hauptsächlich im Zusammenhang mit den Primärsystemen vorzufinden sein.

Entscheidend ist es daher, mögliche Sicherheitsrisiken schon in der Testphase zu erkennen und entsprechende Maßnahmen zu entwickeln, die den Risiken entgegen wirken. Die in diesem Beitrag vorgestellte Bewertung und Klassifikation möglicher Angreifer und Angriffsarten ist der erste Schritt dieses Vorhabens und damit eine wesentliche Basis für die anstehende Sicherheitsevaluation in der Test- und Modellregion Ingolstadt. Ausgehend von dieser Analyse kann möglichen Bedrohungen mit geeigneten Schutzmechanismen entgegen gesteuert und zur Akzeptanz der eGK beigetragen werden. Eine hohe Akzeptanz sowohl von Seiten der Leistungserbringer als auch von Seiten der Patienten ist ein wesentlicher Erfolgsfaktor bei der Einführung der elektronischen Gesundheitskarte in Deutschland. Insbesondere Patienten sind durch Schlagworte wie „der gläserne Patient“ verunsichert. Durch die Schaffung von Transparenz kann dieser Unsicherheit entgegen gewirkt werden. Die Sicherheitsevaluation im Rahmen des Projektes „HatSec“ soll dies erreichen und kann somit zum Gesamterfolg der eGK beitragen.

Literaturverzeichnis

[Ec06] Eckert, Claudia (2006): IT-Sicherheit. 4. überarbeitete Aufl., Oldenbourg Wissenschaftsverlag GmbH, München 2006.

[Ge04] Gerloni, Helmar; Oberhaitzinger, Barbara; Reier, Helmut; Plate, Jürgen (2004): Praxisbuch Sicherheit für Linux-Server und -Netze. Carl Hanser Verlag, München Wien 2004.

[Ma07] Mauro, C.; Sunyaev, A.; Leimeister, J. M.; Schweiger, A.; Krcmar, H. (2008): A Proposed Solution for Managing Doctor’s Smart Cards in Hospitals Using a Single Sign-On Central Architecture. In: Proceedings of the Hawaii International Conference on System Sciences (HICSS 41), January 7 – 10, 2008, Big Island, Hawaii.

[Ne99] Nelson, Bill; Choi, Rodney; Iacobucci, Michael; Mitchell, Mark; Gagnon, Greg 1999: Cyberterror – Prospects and Implications. Center for the Study of Terrorism and Irregular Warfare Monterey, CA, 1999. In: http://www.nps.navy.mil/ctiw/files/cyberterror%20prospects%20and%20implications.pdf, zugegriffen am 13.01.2007.

[Sc00] Schneier, Bruce (2000): Secrets & Lies, IT-Sicherheit in einer vernetzten Welt. dpunkt.verlag GmbH, Heidelberg 2004.

[Su07] Sunyaev, A.; Leimeister, J.M.; Schweiger, A.; Krcmar, H. (2007): Die elektronische Gesundheitskarte und Sicherheitsaspekte: Ein Vorschlag zur entwicklungsbegleitenden Sicherheitsevaluation aus Anwendersicht. In: Informatik 2007 - Informatik trifft Logistik, Band 2. Proceedings of Informatik 2007, Bonn, GI - Gesellschaft für Informatik, S. 469-474.