Rechtliche Aspekte der Sicherheit von Patientendaten beim Einsatz eines WLAN

B. Schütze[1)], M. Kroll[2)], T. Geisbe[1)], H.-G. Lipinski[2)], D.H.W. Grönemeyer[1)], T.J. Filler[3)]

1) Universität Witten/Herdecke, Institut für Radiologie und MikroTherapie
Universitätsstr. 140, 44799 Bochum

{schuetze, geisbe, dg}@microtherapy.de

2) Fachhochschule Dortmund, Fachbereich Medizinische Informatik
Emil-Figge-Str. 42, 44227 Dortmund

{michael.kroll, lipinski}@fh-dortmund.de

3) Universität Münster, Institut für Anatomie
Vesaliusweg 2 – 4, 48149 Münster

klinische.anatomie@uni-muenster.de

Abstract: In der aktuellen Rechtsprechung hat der behandelnde Arzt die Verantwortung für die Sicherheit der ihm anvertrauten Patientendaten. Ob die ihm zur Verfügung gestellten technischen Lösungen, z.B. Wireless LAN (WLAN), Handheld, Laptop etc. diesen Anforderungen an die zu erhaltende Sicherheit der Patientendaten durch ihre technischen Lösungen gerecht werden, kann der Arzt nicht beurteilen und muss gegenwärtig auf den Sachverstand der Entscheidungsträger vertrauen. Hier ist eine Änderung der geltenden Rechtsprechung zu fordern.

1. Einleitung

Die Verwendung drahtloser Netze findet im medizinischen Alltag, insbesondere in deutschen Kliniken, immer mehr Einzug. Den Entscheidungsträgern (Verwaltungsdirektoren, IT-Leiter, Chefärzte, ...) ist hierbei i.d.R. nicht bewusst, dass bei diesem Einsatz oft die Sicherheit der Patientendaten beeinträchtigt wird. Ebenso ist vielen Ärzten nicht bewusst, dass die Verantwortung, und damit die Haftbarkeit, für die Sicherheit der Patientendaten nicht allein bei der Klinikdirektion oder den Chefärzten liegt, sondern zu großen Teilen auch beim behandelnden Arzt selbst. In dieser Arbeit soll eine Einführung in die zurzeit geltende Rechtsprechung gegeben werden, sowie einige Unsicherheiten im Betrieb eines Wireless LANs aufgezeigt werden.

2. Methodik

Basierend auf einer Recherche in den in der Telemedizin relevanten deutschen Gesetzen erfolgte eine Darstellung des aktuellen Stands der Verantwortlichkeiten der Sicherheit der Patientendaten beim Einsatz telematischer Methoden in der Medizin.
Ausgehend von den daraus resultierenden Schlussfolgerungen wurde eine Recherche mittels des Internets über vorhandene Sicherheitsprobleme im Bereich Wireless LAN durchgeführt.

3. Ergebnisse

3.1 Gesetzeslage

Nach §10 der Musterberufsordnung (MBO) für deutsche Ärztinnen und Ärzte hat jeder Arzt über die in Ausübung seines Berufes gemachten Feststellungen und getroffenen Maßnahmen die erforderlichen Aufzeichnungen zu machen.[Bn97] Die Dokumentationspflicht ist somit eine standesrechtliche Berufspflicht. Die Musterberufsordnung stellt jedoch nur ein Satzungsrecht, nicht jedoch eine bundeseinheitliche Rechtsgrundlage dar.
Bundesweit gültige Bestimmungen zur Dokumentation des Behandlungsprozesses sind jedoch mit §43 Abs.1 der Verordnung über den Schutz durch ionisierende Strahlen (StrISchV, Strahlenschutzverordnung), §28 Abs.2 der Verordnung über den Schutz vor Schäden durch Röntgenstrahlen (RöV, Röntgenverordnung), §10 Abs.1 des Gesetzes zur Bekämpfung der Geschlechtskrankheiten (GeschlKrG) und §37 Abs.3 des Gesetzes zum Schutze der arbeitenden Jugend (JArbSchG, Jugendarbeitsschutzgesetz) gegeben. In Berlin ist zudem auf die Krankengeschichtenverordnung (KSVO) hinzuweisen. In diesen Vorschriften ist die Dokumentationspflicht zwar nur für einzelne Teilbereiche der Behandlung oder für bestimmte Rechtspersonen vorgesehen, jedoch ist in der Rechtssprechung die Verpflichtung des Arztes zur Dokumentation seiner Tätigkeiten bei jeder Behandlung allgemein anerkannt.
Für den behandelnden Arzt und dementsprechend tätig werdenden Personenkreis gilt nach §53 Ab2. 1 Strafprozessordnung (StPO) ein Zeugnisverweigerungsrecht und ergänzend hierzu ein Beschlagnahmeverbot nach §97 Abs.1 der StPO. Aus diesem Beschlagnahmeverbot ergibt sich zudem aus §103 Abs.1 StPO ein eingeschränktes Durchsuchungsrecht für Arztpraxen. Das Beschlagnahmeverbot nach §97 StPO gilt jedoch nur, wenn sich die geschützten Gegenstände bzw. Daten im Gewahrsam des Arztes, d.h. innerhalb der Räumlichkeiten der ärztlichen Tätigkeit, befinden und der Arzt diese Gegenstände (Daten) aufgrund des Vertrauensverhältnisses zwischen Arzt und Patient erlangt hat: der Arzt muss die tatsächliche „Sachherrschaft“ ausüben. D.h. es gilt nicht für Daten, die mittels WLAN übertragen und von Außenstehenden „erlauscht“ werden können.
In §9 Abs. 1 MBO wird vorgeschrieben, dass der Arzt über das, was ihm in seiner Eigenschaft als Arzt anvertraut worden ist, zu schweigen hat. Dieses Satzungsrecht wird durch §203 Abs.1 des Strafgesetzbuches (StGB) bestätigt. Danach wird jeder Arzt, der unbefugt ein fremdes, namentlich ein zum persönlichen Lebensbereich gehörendes

Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis offenbart, das ihm als Arzt anvertraut oder sonst bekannt gegeben worden ist, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Standesrechtlich kann die Verletzung der ärztlichen Schweigepflicht sogar zum Widerruf der ärztlichen Approbation führen.
Die Möglichkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten wird durch die Datenschutzgesetze des Bundes, der Kirchen und der Länder stark reglementiert. Die jeweiligen Länder haben für den medizinischen Bereich eigene Gesetze, wobei für Arztpraxen einheitlich das Bundesdatenschutzgesetz gilt. Eine Übersicht über die für Krankenhäuser geltende Gesetze gibt die folgende Tabelle:[He00]

Bundesland	Private Krankenhäuser	Krankenhäuser des Bundes	Krankenhäuser des Landes
Baden Württemberg	LKHG	LKHG	LKHG
Bayern	LKHG	LKHG	LKHG
Berlin	LKHG	LKHG	LKHG
Brandenburg	LKHG	LKHG	LKHG
Bremen	KHDSG	BDSG	KHDSG
Hamburg	LKHG	LKHG	LKHG
Hessen	LKHG	LKHG	LKHG
Mecklenburg-Vorpommern	LKHG	LKHG	LKHG
Niedersachen	BDSG	BDSG	LDSG
Nordrhein-Westfalen	GDSG	BDSG	GDSG
Rheinland-Pfalz	LKHG	LKHG	LKHG
Saarland	LKHG	LKHG	LKHG
Sachsen	LKHG	LKHG	LKHG
Sachsen-Anhalt	BDSG	BDSG	LDSG
Schleswig-Holstein	BDSG	BDSG	LDSG
Thüringen	LKHG	LKHG	LKHG

Tabelle 1: Gesetzgebung und Datenschutz in der Medizin

Legende:

BDSG	Bundesdatenschutzgesetz,	GDSG	Gesundheitsdatenschutzgesetz,
LDSG	Landesdatenschutzgesetz,	LKHG	Landeskrankenhausgesetz
KHDSG	Krankenhausdatenschutzgesetz	KHDsV	Krankenhausdatenschutzverordnung

Die zentrale Aussage dieser Gesetze ist im Prinzip identisch; es existiert ein generelles Verbot der Datenerhebung, ausgenommen ein anderes Gesetz erzwingt die Datenerhebung. Eine Konsequenz daraus ist auch, dass die bei der Behandlung anfallenden Patientendaten nur digital erfasst und bearbeitet werden dürfen, wenn der Patient schriftlich darin eingewilligt hat. Laut Bundesdatenschutzgesetz sind Daten im Gesundheitswesen sogar als besonders schützenswert anzusehen. Für die Übermittlung der Patientendaten mittels digitaler Methoden (eMail, WLAN, etc.) ist daher ein entsprechender Schutz anzuwenden. Für die Einhaltung der betreffenden Datenschutzgesetze ist dabei die Stelle und die Person verantwortlich, bei der die personenbezogenen Daten erhoben und digital gespeichert bzw. verarbeitet werden, d.i. der behandelnde Arzt.
So entsteht hier der Zwiespalt mit der ärztlichen Verantwortung auf der einen Seite, und den mangelnden Einflussmöglichkeiten auf die eingesetzte WLAN-Technologie auf der anderen Seite.

3.2 Sicherheit im Wireless LAN / IEEE 802.11

Die Übertragung von Patientendaten mittels Funkwellen in einem WLAN beinhaltet ein Grundproblem: Funkstrahlung breitet sich gleichmäßig in alle Richtzungen aus und meistens strahlen die WLAN-Funkstrahlen sogar weiter, als der Betreiber es möchte. D.h. ein potentieller Angreifer muss sich nur in der Nähe des WLAN befinden, um Zugriff auf dessen Signale und damit die übertragenen Daten zu erhalten. Daraus resultiert die Folgerung, dass ein WLAN gegen Missbrauch geschützt werden muss. Dies kann nur durch die Methoden der Kryptographie geschehen, da eine Authentifizierung durch MAC- oder IP-Adressen leicht zu umgehen ist.
Der aktuelle Standard IEEE 802.11 verwendet als Verschlüsselungsmethode das „Wired Equivalent Privacy“ (WEP). WEP benutzt RC4, ein symmetrisches Verschlüsselungsverfahren, welches zu den sogenannten Stromchiffren gehört. Ein Startwert („seed“) initialisiert einen Pseudozufallsgenerator und das System erzeugt für jedes zu übertragende Byte einer Nachricht eine neue Zufallszahl. Das verschlüsselte Byte ergibt sich dann durch eine XOR-Verknüpfung mit der Zufallszahl. Die Entschlüsselung verläuft analog, wobei der Empfänger denselben Startwert wie der Sender benutzt.
Scott Fluhrer, Itsik Mantin und Adi Shamir haben bereits Ende Juli 2001 gravierende Sicherheitslücken im Standards IEEE 802.11 festgestellt.[Wc] Basierend auf diesen Erkenntnissen hat ein Student der Rice University zusammen mit zwei AT&T-Labs-Angestellten den 128-Bit-Schlüssel herausgefunden und damit die WEP-Verschlüsselung überwunden.[Go01a] WEP ist der Datensicherheitsstandard für WLANs nach IEEE 802.11. Durch das „RC4 Fast Packet Keying“ wurde diese Sicherheitslücke zwar geschlossen, ob und wann Hersteller die WEP-Verbesserung in ihre WLAN-Produkte einfließen lassen oder ob diese Verbesserungen schon umgesetzt wurden, kann der verantwortliche Arzt jedoch kaum überprüfen.[Go01b] Um die Sicherheit weiter zu erhöhen, implementiert der Standard IEEE 802.1x das Extensible Authentication Protocol (EAP, RFC 2284) und greift für die Authentifizierung auf einen zentralen RADIUS-Server (RFC 2138) zu.[Ie02]
Die amerikanische Colorado State University untersuchte die vorhandenen Möglichkeiten, Authentifizierung und Zugangskontrolle mit oder ohne Unterstützung

von 802.1x zu gewährleisten. Der Studie zufolge behebt 802.1x mehrere der bekannten Sicherheitsprobleme von WEP. Doch andererseits kommt die Studie zu der Erkenntnis, dass auch 802.1x diverse Sicherheitsmängel aufweist.[Ba02] Zu einem ähnlichen Schluss kommen die Forscher William Arbaugh und Arunesh Mishra von der Universität Maryland. Sie haben in ihrer Studie herausgefunden, dass 802.1x erhebliche Schwächen aufweist.[MA02]
Die Projektgruppe „Local Wireless Communication“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hat die Zeitspanne wie auch die benötigte Datenmenge untersucht, die benötigt wird, um einen erfolgreichen Angriff auf ein durch WEP-Verschlüsselung geschütztes WLAN durchzuführen:[Lw02]

Übertragungsgeschwindigkeit➔ Datenmenge⬇	5 Mbit/s	1 Mbit/s	0,1 Mbit/s
0,95 GB	3 min	16 min	2,70 h
1,91 GB	7 min	33 min	5,43 h
2,86 GB	10 min	49 min	8,14 h
3,81 GB	13 min	65 min	10,84 h
5,72 GB	20 min	98 min	16,27 h
7,63 GB	26 min	130 min	21,70 h
11,44 GB	39 min	195 min	32,54 h
15,26 GB	52 min	260 min	43,41 h

Tabelle 2: Dechiffrierung der mittels WEP verschlüsselten Daten in Abhängigkeit der Übertragungsgeschwindigkeit

Im Herbst 2003 soll der Standard IEEE 802.11i verabschiedet werden, welcher den Einsatz des Advanced Encryption Standard (AES) vorsieht.[HM03] Zur Schlüsselverwaltung und –verteilung für AES setzt IEEE 802.11i wiederum IEEE802.1x voraus. Leider haben Kryptoanalytiker einige algebraische Eigenschaften von AES und verwandten Verfahren entdeckt, die AES designbedingt angreifbar erscheinen lassen.[CP02] Zur Zeit ist ein realistischer Angriff basierend auf diesen Erkenntnissen noch nicht durchführbar, bei der stetigen Weiterentwicklung von Mathematik und Rechnerleistung ist ein erfolgreicher Angriff auf AES nur eine Frage der Zeit.

4. Diskussion

Die behandelnden Ärzte haben keinen Einfluss auf die eingesetzte Technologie. Weiterhin kann von keinem Arzt erwartet werden, sich zusätzlich zu seinem eigenen Fachgebiet in den fachfremden, komplexen Bereich der Sicherheit von Computeranwendungen einzuarbeiten, damit er bewusst eine Entscheidung für oder gegen den Einsatz der ihm zur Verfügung gestellten technologischen Hilfsmittel treffen kann. Darüber hinaus sind seine Entscheidungsmöglichkeiten gegen eine neue Technik

oftmals praktisch beschränkt. Andererseits lastet auf diesen Ärzten die rechtliche Verpflichtung, für die Sicherheit der ihnen anvertrauten Patientendaten zu haften.
Hier ist der Gesetzgeber gefordert, die rechtliche Verantwortung von den Ärzten zu nehmen und beispielsweise auf die entsprechenden Entscheidungsträgern (z.B. Verwaltungsdirektoren, IT-Leiter, ...) zu verlagern. Zugleich muss auch vom Gesetzgeber anerkannt werden, dass es in einer vernetzten Gesellschaft keinen hundertprozentigen Schutz von Daten geben kann. Hier sollte in der medizinischen Rechtsprechung das in den anderen Bereichen der Jurisdiktion geltende „in dubio pro reo“ eingeführt werden: wurden entsprechende Anstrengungen zum Schutz der Daten durchgeführt, sollte im Sinne einer verbesserten Behandlungsqualität eine Datenkommunikation erlaubt sein und bei einer stattgefundenen Kompromittierung der Sicherheit der Patientendaten nicht von einer strafbaren Handlung des behandelnden Arztes bzw. von einer haftungsrechtlich relevanten Straftat ausgegangen werden.

Literaturverzeichnis

[Ba02] Baily, S.: Is IEEE 802.1X Ready for General Deployment? http://rr.sans.org/casestudies/deployment.php, 07.04.2002

[Bn97] Bundesverband niedergelassener Fachärzte Deutschland e.V. – BNF: Musterberufsordnung für Ärzte, http://www.bnf.de/dokumente/mbo.php3, Mai 1997

[CP02] Courtois N. T.; Pieprzyk J.: Cryptanalysis of Block Ciphers with Overdefined Systems of Equations, http://eprint.iacr.org/2002/044/, November 2002

[Go01a] Golem.de: http://www.golem.de/showhigh.php?file=/0108/15270.html&wort[]=WEP%20Verschlüsselung, 10.08.2001

[Go01b] Golem.de: http://www.golem.de/0112/17523.html, 20.12.2001

[He00] Hermeler, A. E.: Rechtliche Rahmenbedingungen der Telemedizin, Verlag C. H. Beck, 2000 ISBN 3 406 46875 6

[HM03] Hoff S.; Mohn H. P.: 802.11i unter der Lupe, LANline, 3, 56 - 60, 2003

[Ie02] IEEE: http://www.ieee802.org/1/pages/802.1x.html, 22.03.2002

[Lw02] Projektgruppe „Local Wireless Communication“: Bundesamt für Sicherheit in der Informationstechnik (BSI), Sicherheit im Funk-LAN (WLAN, IEEE 802.11), http://www.bsi.de/fachthem/funk_lan/wlaninfo.pdf; July 2002

[MA02] Mishra A.; Arbaugh W.A.: An Initial Security Analysis of the IEEE 802.1X Standard, http://www.cs.umd.edu/~waa/1x.pdf, 06.02.2002

[Wc] Wireless Communication Austria: http://www.wireless.co.at/News.asp?NewsID=135,