WLAN im Gesundheitswesen
Sicherheitslücken und rechtliche Implikationen

Minh-Huy Tran-Huu[1], Johannes Ranke[2], Hans-Bernd Bludau[1]

[1]Universität Heidelberg
Innere Medizin II
[2]TU Darmstadt
GK „Infrastruktur für den elektronischen Markt“

tranhuu@uni-mannheim.de
hans-bernd.bludau@med.uni-heidelberg.de
johannes_ranke@yahoo.de

Abstract: Der Einsatz drahtloser Netzwerke findet immer mehr Befürworter, da sich so die kostenintensive und oft umständliche Verkabelung vermeiden lässt. Die elektromagnetische Verträglichkeit dieser Technik ist gut und deshalb auch für Krankenhäuser und Praxen interessant. Allerdings ermöglichen Funknetzwerke sogenannten "Wardriveren", die sich problemlos in die Datenübertragung Dritter einloggen, rasch den Zugang zum Netzwerk. Im nachfolgenden Artikel werden im ersten Teil die sicherheits-technischen Aspekte eines Funknetzwerkes, deren Schwachstellen sowie mögliche Vorkehrungen zur Verbesserung der Sicherheit aufgezeigt. Im zweiten Teil des Artikels werden dann die rechtlichen Grundlagen sowie die möglichen Implikationen für Netzwerkbetreiber referiert.

1. Einleitung

‚Lauschangriff aus der Luft: Wer funkt, spricht laut. Der kabellose Austausch von Daten, wie ihn zum Beispiel Computernutzer über Funknetzwerke betreiben, kann fast so einfach wie ein Gespräch auf der Straße mitgehört werden.’ [Rh02].
Solche und ähnliche Meldungen kann man zunehmend in den Medien lesen (z.B. [VS02]). Was sich eher nach einem Science Fiction Szenario anhört als nach Realität, ist jedoch gar nicht weit hergeholt. Denn mit zunehmender Verbreitung entsprechender Funknetze, den sogenannten Wireless Local Area Networks, kurz WLANs, steigt die Gefahr tatsächlichen Missbrauches.

2. Technische Aspekte

Das WEP (Wired Equivalent Privacy) ist ein Verschlüsselungsmodul im Funklan, das mit einem Algorithmus arbeitet. Der WEP-Algorithmus arbeitet einfach: Der RC4, Rons Cipher 4, ist ein Pseudozufallsgenerator, der von einem WEP Schlüssel und einem Initialisierungsvektor gespeist wird und dem WEP Algorithmus den "zufälligen" Schlüsselstrom liefert. Dieser wiederum wird mit Hilfe der XOR-Operation mit dem Klartext verrechnet, im Folgenden mit geXORt bezeichnet.

Der RC4 Algorithmus arbeitet beim WEP mit 64 bzw. 128 Bit, wovon 24 Bit den Initialisierungsvektor bilden. Die restlichen 40 bzw. 102 Bit werden von den Benutzern selbst festgelegt, wobei alle Schlüssel in einem Funknetzwerk identisch sein müssen, d.h. jeder Client und Access Point hat den gleichen Key (Shared Key). Zum zweiten wird bei WEP ein Teil des 64/128 Bit Schlüssels als Klartext übermittelt. Dann folgt der eigentliche, verschlüsselte Block mit Daten und Prüfsumme.
Mit dem 24 Bit Initialisierungsvektor und dem "geheimen" WEPkey wird der Pseudozufallsgenerator RC4 gestartet. Der RC4 Algorithmus liefert dem WEP Algorithmus Zufallszahlen, die mit dem Klartext und dem zum Klartext zugehörigen ICV (Integrity Check Value) geXORt werden. Übertragen wird dann der verschlüsselte Text, während der Initialisierungsvektor als Klartext übermittelt wird. Zum Entschlüsseln wird der RC4 wieder mit dem WEP Schlüssel und dem Initialisierungsvektor gestartet. Dieser Strom wird mit dem übermitteltem Strom geXORt, so dass der Klartext lesbar ist. Dabei wird auch die Datenintegrität überprüft.
Der RC4 wurde 1987 von Ron Rivest erfunden. RC4 steht für Rivest Cipher, manchmal auch als Rons Code bezeichnet. RC4 war geheim und konnte nur nach der Unterzeichnung eines Geheimhaltungsabkommens eingesehen werden. Im September 1994 wurde der Quellcode in der ‚Mailingliste Cypherpunks' anonym veröffentlicht. Der RC4 arbeitet im OFB Modus, das heißt, der Schlüsselstrom ist unabhängig vom Klartext.

2.1. Schwachstellen und Angriffsmöglichkeiten

- Die Folgen zu kurzer Schlüssel

Ein Schwachpunkt im WLAN ist der Initialisierungsvektor. Schon nach 2^{24} Übertragungen wiederholt sich der Schlüssel. Das sind 16777216 Pakete. In der Praxis bedeutet das, dass man nur circa 15GB Daten abhören muss, was circa 5 Stunden dauert [BS02]. Teile vom Schlüssel kann man bereits mit Sniffer-Angriffen bekommen, da ja der Initialisierungsvektor unverschlüsselt übertragen wird.

- Known Plaintext Attack (Angriff mit bekanntem Klartext)

Bei der Known Plaintext Attack schickt der Angreifer einem Benutzer im WEP-WLAN eine EMail (z.B. Spam) mit einer beliebigen Nachricht und verfolgt dabei den Netzwerkbetrieb. Ihm unbekannte Daten kann der Angreifer dabei aus der bekannten Struktur von IP-Paketen und bekannten festen Werten ableiten.

- Cyclic Redundancy Check , kurz CRC, (Fehlerkorrektursystem bei der Übertragung digitaler Daten)

Durch das Anfügen der CRC-Summe an die Datenpakete sollen sowohl zufällige als auch mutwillige Störungen auf dem Übertragungswege erkannt werden [BS02]. Gegen zufällige Störungen hilft diese Methode tatsächlich; denn Fehler werden mit hoher Wahrscheinlichkeit erkannt. Werden dagegen gezielte Bits in den Chiffredaten gestört, das wegen der einfachen XOR-Struktur des Stromchiffrier-Algorithmus eine Störung der entsprechenden Bits im Klartext zufolge hat, kann auch die verschlüsselte CRC-Summe

modifiziert werden, so dass der Angriff beim Empfänger nicht entdeckt wird. Grund hierfür ist die Linearität [WO02] der CRC-Summe und die XOR-Struktur des Stromchiffrier-Algorithmus.

- Die Schwachstelle von RC4

Obwohl der RC4 Algorithmus nie offiziell veröffentlich wurde, ist dieser Algorithmus bekannt. Fluhrer, Mantin, und Shamir [FMS01] entdeckten, dass aus den ersten Zufallszahlen der Anfangswert einer RC4 S-Box ermittelt kann.

- Initialisierungsvektor

Hier liegt die Schwachstelle in der Implementation. Eigentlich müsste der Initialisierungsvektor eine "Zufallszahl" sein. Aber bei vielen Produkten hat der erste Initialisierungsvektor den Wert "1", der dann inkrementiert wird.

2.2. Verbesserung der Sicherheit in Funknetzwerken

Es existieren verschiedene Soft- und Hardware Lösungen, die bei den oben aufgeführten Problemen Abhilfe schaffen können. Allerdings muss auch bei diesen Lösungen mit spezifischen Sicherheitslücken gerechnet werden.

- Kerberos

Kerberos ist ein Authentifizierungsprotokoll, das im Rahmen des Athena Projektes am MIT, dem Massachusetts Institute of Technology, entwickelt worden ist [KN93]. Es ist dazu konzipiert, in unsicheren Netzen zu fungieren. Eine zentrale Funktion spielt dabei der sogenannte Ticket Granting Server, kurz TGS, mit dem sich Clients und Server gegenseitig authentisieren können. Weitere Sicherheitsaspekte werden durch die begrenzte Gültigkeitsdauer der einzelnen Tickets und Sessionkeys erreicht. Kerberos hat mindestens eine Schwachstelle: den Kerberosserver selbst. Denn liegt eine physikalische Zugriffsmöglichkeit darauf vor, müssen alle Passwörter geändert werden.

- IPsec (IP Security)

IPsec ist die Verschlüsselungsschicht von IPv6, welche aber auch mit IPv4 verwendet werden kann. Sie schützt mit Verschlüsselungstechnik vor unbefugtem Lesen und garantiert die Echtheit der Nachricht bezüglich des Inhalts und des Absenders durch Hash-Algorithmen. Zum Verschlüsseln nimmt man meistens 3DES (Tripple DES), jedoch können durch die flexible Struktur von IPsec auch andere Algorithmen verwendet werden. IPsec hat zwei Modi:

Im Transportmodus werden nur die Nutzdaten verschlüsselt, der IP Header wird nicht verändert. Der Transportmodus wird bei der Übertragung von Informationen verwendet, bei denen die Echtheit der Nachricht nicht oberste Priorität hat.

Der Tunnelmodus nutzt man im VPN (Virtual Privat Network). Bei diesem Modus wird alles verschlüsselt, sowohl die Nutzdaten als auch der IP Header. Die verschlüsselten IP Header und Daten werden zwischen dem ESP (Encapsulating Security Payload) Header und dem ESPTrailer eingeschlossen.

- PPTP (Point to Point Tunneling Protocol)

PPTP wird unter Windows ‚VPN Adapter' genannt. Die Pakete werden in GREv2 (Generic Routing Encapsulation Protocol V2) versendet, wobei je Kommunikationspaar nur ein Tunnel aufgebaut werden kann. Bereits 2001 wurden die, vorab von Bruce Schneier beschriebenen Schwachstellen von PPTP, durch Jochen Eisinger [Sc99] in einer praktischen Anwendung umgesetzt. Mit seiner Software zeigte er, wie leicht die Schwäche der häufig eingesetzten MS-CHAPv2 (Microsoft Challenge/Reply Handshake Protocol)-Authentifizierung ausgenutzt werden kann. Diese Schwäche reduziert letztlich die in Frage kommenden Passwörter um den Faktor 2^{16}.[Si01]

- Fast Packet Keying

Fast Packet Keying von der Firma RSA bildet aus einem konstanten Schlüssel und der Sendeadresse einen individuellen 104 Bit langen Initialisierungsvektor. So wiederholen sich die Initialisierungsvektoren erst nach 2^{103} Paketen.

- WEPplus

Die Firma Lucent verändert mit ‚WEPplus', das kompatibel zu WEP ist, den Algorithmus zum Erzeugen von Initialisierungsvektoren, die allerdings immer noch als Klartext übertragen werden.

2.3. Erste Schritte zu sichereren Funk-Netzwerken

- Werkseitige Passwortvorgaben ändern

Diese Möglichkeit muss am Access-Point und bei allen Clients vorgenommen werden. Die ESSID bzw. SSID ((Extended) Service Set Identity = Netzwerkname) sollte keine Rückschlüsse auf Firma oder Netzwerk zulassen. Unzureichende Standardnamen wie "WLAN" sollten geändert werden, obwohl die meisten APs ihre SSID senden und diese dadurch ausspioniert werden können. Lassen sich die SSID-Broadcasts am AP abschalten (Closed-System-Modus), sollten sie deaktiviert werden. Durch Umbenennen der SSID werden zumindest zufällige Anmeldungen verhindert. Dennoch bleibt die Gefahr, dass die SSID mit Tools wie z.B. NetStumbler ausspioniert werden kann. Daneben sollte auch regelmäßig das Passwort zur AP-Konfiguration geändert werden.

- WEP-Verschlüsselung verwenden

Mit dem Einsatz von WEP wird durch die Verschlüsselung zumindest eine gewisse Barriere errichtet, die Gelegenheitslauscher abhält. Ein Einbruch lässt sich jedoch nicht verhindern, sondern nur erschweren und hinauszögern. Zudem hat WEP noch viele

andere Schwachstellen. Zum Beispiel muss sich zwar der Client gegenüber dem AP authentifizieren, jedoch nicht umgekehrt, was eine Man-in-the-Middle-Attack ermöglicht.

- MAC (Medium Access Control)-Adressen filtern

Viele APs speichern die zugelassenen MAC-Adressen in einer Liste, die der Administrator einmal erstellt und dann pflegt. Nur zugelassene MAC-Adressen dürfen sich an den Basisstationen anmelden. Zwar können auch Sie gefälscht werden, doch muss zuvor ein Angreifer mindestens eine echte MAC-Adresse kennen, um sie nutzen zu können.

- DHCP (Dynamic Host Configuration Protokoll)

DHCP vergibt im Netzwerk auf Anfrage automatisch eine IP-Adresse. Im Funk-LAN sollte dieses Protokoll abgeschaltet sein. Zudem sollte man den IP-Adressraum kleinstmöglich wählen. Die Verwendung statischer Adressen, die nicht den Standartwerten entsprechen, erschweren das Eindringen.

3. Rechtliche Aspekte

Entsprechend der rechtlichen Grundlagen können unterschiedliche Positionen betrachtet werden. Zum einen ist die rechtliche Position des Netzwerkbetreibers zu beachten, der einerseits den Zugang zum Internet erlaubt, andererseits sensible Daten innerhalb seines Krankenhausinformationssystems zu schützen hat. Zudem wird dem Abhörenden eine Strafverfolgung angedroht aber auch der Person Schutzwürdigkeit zugesprochen, deren „Identität“ durch den unberechtigten Zugang zum Netz übernommen wird.

3.1 Daten und Systemsicherungspflichten beim Einsatz drahtloser Netzwerke im Gesundheitswesen

- Verhinderung von unbefugten Internetverbindungen

Stellen Krankenhausträger WLAN-Netze zur Verfügung, die auch unbefugten Dritten mit geringen technischen Aufwandes den Zugang ins Internet ermöglichen, sind Sicherungsmaßnahmen vor allem aus ökonomischen Gesichtspunkten vorzunehmen. Zu rechtlichen Problemen könnte das unberechtigte Einloggen ins Internet über einen drahtlosen Access point führen, wenn statische IP-Adressen automatisch dem „Wardriver“ zugewiesen werden, die üblicherweise den Rechnern des Krankenhausträgers oder sogar denen einzelner Mitarbeitern zugeordnet sind. Denn schließt der „Wardriver“ dann im Internet Verträge ab, könnten diese dem Krankenhausträger oder einem Mitarbeiter zugerechnet werden. Die Betroffenen könnten zwar im Prozess behaupten, dass sie keine Vertragserklärungen abgegeben haben, so dass der Geschäftspartner den Vertragsschluss beweisen müsste. Nach dem

derzeitigen Rechtsstand ist aber nicht geklärt, welche Anforderungen Gerichte an den Beweiswert von Willenserklärungen im Internet stellen.

Neben der unberechtigten Geltendmachung von Vertragsansprüchen besteht für die Mitarbeiter die Gefahr, dass sie fälschlicherweise verdächtigt werden, strafbare Handlungen über das Internet begangen zu haben, wenn der „Wardriver“ Internetdateien unter Verletzung des Urheberrechtes oder mit kinderpornographischem Inhalt über die statische IP-Adresse eines Mitarbeiterrechners heruntergeladen hat. Auch hier könnte sich der Mitarbeiter zwar einer Bestrafung entziehen, indem er im Prozess vorträgt, dass sich möglicherweise fremde Personen in das unsicherer Systeme eingeloggt haben. Der gesellschaftliche und möglicherweise soziale Schaden für ihn kann jedoch nicht zu hoch bemessen werden.

Werden Mitarbeiter in Vertragsprozesse und falsche Verdächtigungen hineingezogen, ist ihre Privat- und Intimsphäre betroffen. Da diese aber durch die allgemeine Fürsorgepflicht des Arbeitgebers zu schützen ist [Ri98], folgt für die Krankenhausträger, dass sie das unberechtigte Einloggen Dritter unter IP-Adressen der Mitarbeiter verhindern müssen. Die genauen Maßnahmen könnten sich dabei aus dem Arbeits- oder Tarifvertrag ergeben. Jedoch sehen diese derzeit regelmäßig meist keine technischen Sicherheitsanforderungen vor.

Neben dem allgemeinen Fürsorgerecht des Arbeitgebers ließe sich eine solche Verpflichtung eventuell auch auf § 9 BDSG stützen. Danach haben öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, technische und organisatorische Maßnahmen zu treffen, die den in der Anlage zum BDSG beschrieben Anforderungen entsprechen. Aus den einzelnen Sicherungspflichten der Anlage ergibt sich zwar nicht ausdrücklich, dass das unberechtigte Einloggen unter statischen IP-Adressen zu verhindern ist. Aus deren Sinn kann man aber ableiten, dass unwahre Tatsachen nicht einer fremden Person zugeordnet werden sollen.

- Verhinderung von Abhörmaßnahmen

Das Abhören des nicht öffentlich gesprochenen Wortes ist gem. § 201 StGB strafbar. Gleiches gilt für sonstige elektronische Nachrichten nach § 202a StGB, wenn sie gegen unberechtigten Zugang (wie etwa WEP) gesondert geschützt sind.[DSK02] Die Strafbarkeit resultiert aus dem verfassungsmäßig gewährleisteten Recht des Fernmeldegeheimnisses, das dem Staat auch die Verpflichtung auferlegt, seine Bürger vor Verletzungen Dritter zu schützen.

Aus dieser Schutzpflicht heraus hat der Gesetzgeber mit § 87 Nr. 1 TKG auch eine gesetzliche Regelung geschaffen, welche die Telekommunikationsanbieter verpflichtet, Sicherheitsmaßnahmen zur Wahrung des Fernmeldegeheimnisses zu schaffen. Die Verpflichtung aus § 87 TKG trifft jedoch nur diejenigen TK-Anbieter, die TK-Dienste geschäftsmäßig erbringen. Deshalb sind Schutzpflichten nach § 87 TKG nur dann zu ergreifen, wenn die TK-Dienstleistung gegenüber Dritten angeboten wird und auf eine gewisse Dauer angelegt ist. Auf die Entgeltlichkeit kommt es indes nicht an.[Eh00]

Werden WLAN-Netze im Krankenhausbetrieb nur den Angestellten des Krankenhauses zur Erfüllung ihres Arbeitsvertrages zur Verfügung gestellt, kann nicht von einer Angebotsleistung an Dritte ausgegangen werden. Denn die Telekommunikationsleistung wird nur zum Eigenbedarf erbracht. Anders ist der Sachverhalt jedoch dann zu beurteilen, wenn Patienten oder Angestellten der Zugang in das WLAN-Netz auch zu privaten Zwecken ermöglicht wird. Denn gegenüber den Patienten stellt der Zugang in das krankenhausinterne WLAN-Netz stets ein Angebot gegenüber Dritten dar, und auch bei der privaten Nutzung der Mitarbeiter treten diese nicht mehr als Teil des Unternehmens auf.

Allerdings würde dieses Ergebnis nicht befriedigen, da bei der ärztlichen Tätigkeit eine Fülle von personenbezogenen Patienten- und Mitarbeiterdaten über die WLAN übertragen werden. Aus § 9 BDSG i.V.m. der Anlage ergibt sich jedoch, dass die Übermittlungsebene auch außerhalb geschäftsmäßiger TK-Angebote vor Abhörmaßnahmen zu schützen ist. Denn das BDSG schützt personenbezogene Daten unabhängig davon, ob sie auf der Übertragungsebene übermittelt oder dauerhaft gespeichert werden. Nach Nr. 1 der Anlage zum BDSG ist Unbefugten aber der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren und nach Nr. 2 ist zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Daneben ließe sich eine Schutzpflicht der Patienten und Mitarbeiterdaten auf der Übertragungsebene auch aus der allgemeinen Fürsorgepflicht des Arbeitgebers und aus dem gewohnheitsrechtlich anerkannten Arztgeheimnis ableiten.

- Verhinderung von Zugriffen auf das Zentralsystem

Die rechtliche Verpflichtung zur Sicherung des Zentralsystems ergibt sich aus § 9 BDSG i.V.m. dessen Anlage. Daneben ließe sich eine Sicherungspflicht auch hier aus der allgemeinen Fürsorgepflicht des Arbeitgebers sowie aus dem gewohnheitsrechtlich anerkannten Arztgeheimnis ableiten.

3.2 Umfang der Daten- und Systemsicherungspflichten

Weder aus den gesetzlichen Regelungen des § 87 TKG und § 9 BDSG i.V.m. dessen Anlage, noch aus der allgemeinen Fürsorgepflicht des Arbeitgebers und dem Arztgeheimnis ergibt sich, welche Sicherheitsmaßnahmen genau zu ergreifen sind. Fest steht nur, dass der Umfang der zu treffenden Sicherheitsmaßnahmen grundsätzlich von der Bedeutung der zu schützenden Rechte abhängig ist.

Andererseits ist darauf hinzuweisen, dass von den Krankenhausträgern nicht alles nur Erdenkliche verlangt werden kann, was technisch und organisatorisch für den Schutz der Vertraulichkeit möglich ist. Denn die Schutzmaßnahmen vor Angriffen Dritter sind stets mit den Rechten des Krankenhausträgers auf Ausübung und Entfaltung seiner Eigentumsrechte und seiner wirtschaftlichen Entfaltungsfreiheit abzuwägen. Daher sind

die Verpflichtungen nach dem Wortlaut des § 9 BDSG und § 87 Abs. 1 TKG auf angemessene und zumutbare Vorkehrungen beschränkt.
Das Schaffen angemessener, technischer Vorkehrungen zum Schutz vor Störungen und Angriffen bedarf deshalb stets einer umfassenden und wiederholten Prüfung. Dabei sind die einzelnen Sicherheitsmaßnahmen gegebenenfalls konzeptionell zu verbinden, wenn verschiedene Maßnahmen zusammen eine sicherheitstechnische Aufgabe erfüllen.
Zur Objektivierung des Begriffes der „Zumutbarkeit“ kann von einer zumutbaren Maßnahme ausgegangen werden, wenn Krankenhausträger, die im selben „Marktsegment“ agieren, solche Sicherheitsmaßnahmen durchgeführt haben. Bei den Sicherheitsanforderungen drahtloser Netzwerke in Universitätskrankenhäusern, die eine Größe von ca. 1000 Betten haben, wird man allerdings annehmen können, dass die ab Kapitel 2.2 (Verbesserung der Sicherheit in Funknetzwerken) aufgezeigten Sicherheitsmaßnahmen dem Stand der Technik entsprechen und auch wirtschaftlich zumutbar sind.

3.3 Rechtsfolgen unterlassener Sicherheitsmaßnahmen

Werden angemessene Sicherungspflichten durch den Krankenhausträger unterlassen und führt dies zur Verletzung der Nutzerrechte durch Dritte, kann es zu zivilrechtlichen Schadensersatzforderungen führen, die auf § 823 BGB oder auf § 40 TKG gestützt werden können. Wegen der Schwierigkeit für den Betroffenen zu beweisen, dass seine Rechte aufgrund fehlender Sicherheitsmaßnahmen verletzt wurden, wird in zunehmendem Maße von der Rechtsliteratur gefordert, dass die Verletzung von Sicherheitspflichten generell als Ordnungswidrigkeit zu ahnden ist. Eine solche Möglichkeit sieht zwar § 96 Abs. 1 Nr. 9 TKG für Sicherungspflichten auf der Übertragungsebene bereits vor. Von einer Präzisierung der Sicherungspflichten durch eine Verordnung gem. § 87 Abs. 3 TKG, die als Grundlage zur Ahndung von Sicherheitsmängel gem. § 96 Abs. 1 Nr. 9 TKG dient, wurde jedoch bis dato abgesehen.

4. Zusammenfassung

Die WLAN für mobile Computer findet zunehmend Verbreitung. Auch im Gesundheitswesen ist dies eine Möglichkeit, ein schnelles und einfach zu installierendes Netzwerk aufzubauen. Allerdings müssen dezidierte Sicherheitsaspekte dieser Technik berücksichtigt werden, um die sensiblen Daten vor Fremdzugriffen zu schützen. Um die Sicherheit im WEP zu erhöhen, hat das IEEE (Institute of Electrical and Electronics Engineers) eine entsprechende Arbeitsgruppe gegründet.
Die vorliegende Arbeit hat die verbreitetsten Techniken zur Sicherung von Funknetzwerken zusammengefasst und auf die Notwendigkeit einer intensiven Benutzerschulung hingewiesen. Sichere Netzwerke sind keine "Alleskönner" und schützen nicht vor unerwünschten ‚Spam-Mails', ‚Emailwürmern', ‚Trojanern' oder ‚Viren'. Selbst in VPNs (virtuellen privaten Netzwerken) sollten für die Übertragung wichtiger Daten nur derzeit "sichere" Protokolle verwendet werden. Doch auch bei Verwendung sogenannter Sicherheitsstandards muss die Möglichkeit eines externen Zugriffs berücksichtigt und den Nutzern kommuniziert werden.

Die rechtlichen Rahmenbedingungen decken den neu entstandenen Bereich von Funk-LANs ausreichend ab. Allerdings fehlen Präzedenzfälle, so dass eine Empfehlung derzeit eher konservativ ausfällt. Deshalb ist es insbesondere für Krankenhäuser von entscheidender Bedeutung ein Sicherheitskonzept zu entwerfen, das neben der technischen auch die organisatorische Sicherheit mit einschließt und gegebenenfalls über Sicherheitslücken informiert.
Schwierigkeiten bestehen bei der Gewährleistung der Sicherheitsanforderungen in drahtlosen Funknetzen, da diese Luftschnittstelle nicht in dem physischen Machtbereich des Krankenhausträgers steht und er eine Verschlüsselung der Daten nur dann vornehmen kann, wenn die Endgeräte den vom Krankenhausträger genutzten Verschlüsselungsstandard nutzen.
Jedoch wird auch im sichersten Netzwerk immer eine Schwachstelle bleiben: Der Benutzer. Dieser sollte die Möglichkeit eines Fremdzugriffes immer berücksichtigen und in Netzwerken entsprechend vorsichtig mit sensiblen, elektronischen Daten umgehen. Die zunehmende Verbreitung von Funknetzwerken erhöht den Aufklärungsbedarf bezüglich integrierter Sicherheitsstandards und möglicher Sicherheitslücken. Insbesondere im Gesundheitswesen müssen höchste Ansprüche an die Datenintegrität und -sicherheit gestellt werden.

Literaturverzeichnis

[BS02] Bundesamtes für Sicherheit in der Informationstechnik (BSI), Bonn. Sicherheit im Funk-LAN (WLAN, IEEE 802.11), Projektgruppe "Local Wireless Communication", 2002. http://www.bsi.bund.de/fachthem/funk_lan/wlaninfo.pdf. Letzter Zugriff: 30.01.03.

[DSK02] Dornseif, M, Schumann, K., Klein, C. Tatsächliche und rechtliche Risiken drahtloser Computernetzwerke, DuD 2002, 226 f.

[Eh00] Ehmer, Jörg in: Beck`scher TKG-Kommentar, 2. Auflage 2000, § 87 Rdnr. 23.

[FMS01] S. Fluhrer, I. Mantin, A. Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, 8. Annual Workshop on Selected Areas in Cryptography, August 2001. http://www.crypto.com/papers/others/rc4_ksaproc.ps.

[KN93] Kohl, J.; C Neuman, C: The Kerberos Network Authentication Service (V5) RFC 1993, http://www.faqs.org/rfcs/rfc1510.html.

[Rh02] Rhein Zeitung. Funknetzwerk WLAN hat Sicherheitslücken: Lauschangriff aus der Luft. 21.10.02. http://rhein-zeitung.de/on/02/10/21/topnews/lausch.html

[Ri98] Ring, Gehard, Arbeitsrecht, 1.Auflage 1998.

[RW02] Mishra, R.; Argbaugh, W.: An Initial Security of the IEEE 802.1X Standard, Feb 2002. http://www.missl.cs.umd.edu/wireless/1x.pdf

[Si01] Siering, Microsofts PPTP gehackt, c't 16/2001.

[Si02] Sikora, A.: Sicherheit in Wireless LANs, Elektronik, 18/2002, S.44-52. http://www.elektroniknet.de/topics/kommunikation/fachthemen/2002/0027/index.htm#inhalt

[Ss99] Schneier, B: Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2), Springer-Verlag, 1999. http://www.counterpane.com/pptpv2-paper.html.

[VS02] Virtel, M; Sosalla, U: Zeichen für Eingeweihte. Financial Times Deutschland vom 13.12.2002. URL (02.01.03): http://www.ftd.de/ed/we/1039610307420.html

[WO02] Weis, Ohlig: WLAN Security, Fachkongress Wireless Lan, Köln 12.11.2002 http://www.cryptolabs.org/wep/WeisOhligWLANsecurity.pdf