DuD
Datenschutz und Datensicherheit

Tatsächliche und rechtliche Risiken drahtloser Computernetzwerke

Maximillian Dornseif, Kay H. Schumann, Christian Klein

Die Gefahren von Funknetzwerken werden vielerorts beschworen. Wie groß ist das tatsächliche Gefahrenpotential und wie steht das Strafrecht zu Angriffen auf Funknetzwerke?

[FOTO] Maximillian Dornseif

promoviert am Lehrstuhl für Strafrecht der Universität Bonn zum Thema Rechtstatsachen der Computerkriminalität

E-Mail: md@hudora.de

[FOTO] Kay H. Schumann

ist Rechtsreferendar. Er promoviert am Lehrstuhl für Strafrecht der Universität Bonn zum Thema Strafrechtliche Bedeutung von elektronischen Zahlungsmitteln
E-Mail: kayschumann@mac.com

[FOTO] Christian Klein

studiert Informatik an der Universität Bonn und arbeitet Junior Consultant bei der c0re GmbH, Bonn

E-Mail: ck@c0re.23.nu

Einleitung

Über die Risiken von Wave-LANs, wie drahtlose Computernetzwerke nach dem IEEE 802.11 Standard bezeichnet werden, wurde in den letzten Monaten viel berichtet [1]. Das Wort vom *drive-by-hacking* bzw. *war driving* macht die Runde. Methodische Untersuchungen konzentrieren sich bisher allerdings auf die kryptografischen Probleme [2]. Im vorliegenden Beitrag wird die Bedeutung dieser Probleme im Kontext der Protokollmechanismen erklärt und anhand dessen eine strafrechtliche Bewertung vorgenommen. Darüber hinaus werden die Ergebnisse einer Abschätzung der tatsächlichen Bedrohungslage vorgestellt; zu diesem Zweck wurde die Verbreitung und Konfiguration von Wave-LANs in Bonn ermittelt.

1 Problemaufriss

Funkkommunikation unterscheidet sich von kabelgebundener Kommunikation durch das verwendete Übertragungsmedium. Der Zugriff auf übertragene Daten ist bei einem Kabel relativ einfach zu regeln: Wer keinen Zugriff auf das Kabel hat, kann in aller Regel nicht ohne erheblichen Aufwand auf die darüber übertragenen Daten zugreifen.

Das Übertragungsmedium bei drahtloser Kommunikation sind Funkwellen, die sich von einem Sender aus grundsätzlich kreisförmig ausbreiten. Dabei sinkt die Übertragungsleistung quadratisch mit dem Abstand zur Quelle. Innerhalb bebauter Bereiche ist der Ausbreitungsradius geringer und lässt sich die Ausbreitung nur sehr unvollkommen voraussagen.

Auch wenn sich die Ausbreitung durch geschickte Wahl von Antennen und Sendeleistung teilweise kontrollieren lässt, macht die Abdeckungswolke einer drahtlosen Kommunikation in privaten „Netzen“ nicht an Gebäude- oder Grundstücksgrenzen halt. In der Praxis führt das dazu, dass regelmäßig auch von öffentlichem Grund aus der Empfang der drahtlosen Kommunikation einer Institution möglich ist.

Dieses Problem zeigte sich bereits vor einigen Jahren vor der Einführung des DECT-Standards im Zusammenhang mit schnurlosen Telefonen. Ein weithin bekannter Fall sind die abgehörten Telefongespräche des englischen Thronfolgers.

Bei den heute verbreiteten funkbasierten Computernetzwerken auf Basis von IEEE 802.11b sorgen vier Faktoren dafür, dass das Risiko um ein Vielfaches höher ist, als bei schnurlosen Telefonen:

- Die Daten in Computernetzwerken decken eine viel weitere Bandbreite von möglichen Inhalten ab als Telefongespräche.
- Weil die Daten in elektronischer Form vorliegen, sind sie leicht zu speichern und zu filtern bzw. zu durchsuchen.
- Netze ermöglichen potenziell den Zugriff auf wesentlich mehr Informationen. In vielen Fällen ist es möglich, per Wave-LAN eine etwaige „Firewall“ zu umgehen und so Zugang zum internen Firmennetzwerk zu erhalten.
- Während zum Abhören von schnurlosen Telefonen aufwändige Technik nötig ist, reicht bei drahtlosen Computernetzen eine Anpassung der Netzwerksoftware.

Bei unautorisiertem Zugang zu einem Wave-LAN kommen eine Vielzahl von Tatszenarien in Betracht. Hier einige Beispiele:

- **Internetnutzung:** Ein Unberechtigter kann möglicherweise einen fremden Internetzugang nutzen. Das bietet für ihn einen hohen Grad an Anonymität. Neben den entstehenden Kosten fallen alle seine – möglicherweise strafbaren – Handlungen im Internet im Zweifel auf den Anschlussinhaber zurück.
- **Abhören von Kommunikation:** Der Unberechtigte kann die laufende Kommunikation innerhalb des drahtlosen Netzwerkes und möglicherweise auch

innerhalb des Firmennetzwerkes abhören.

- **„Datendiebstahl“:** Dadurch, dass der Unberechtigte „von innen“ auf das Netzwerk zugreift, hat er mit hoher Wahrscheinlichkeit lesenden Zugriff auf innerhalb des Netzes gespeicherte Daten, die von außen nicht abrufbar sind.
- **Datenmanipulation:** Ein Unberechtigter kann möglicherweise gespeicherte Daten oder Daten, die gerade in der Übertragung sind, verändern.

2 Technische Grundlagen

Die heute überwiegend zum Einsatz kommende Technik für drahtlose Netzwerke ist Wireless Ethernet nach dem IEEE Standard 802.11b (Wave-LAN). Diese Netze können als *Ad-Hoc Netzwerk*, bei denen mehrere Computer gleichberechtigt kommunizieren oder im *Managed Mode*, bei dem eine Basisstation den Datenverkehr regelt, betrieben werden. Wir werden uns bei der Beschreibung auf den *Managed Mode* beschränken, da dieser eine wesentlich geringere Komplexität aufweist und – wie wir zeigen werden – wesentlich verbreiteter zu sein scheint.

Im Weiteren wird eine skizzenhafte Beschreibung der technischen Funktionsweise von Wave-LAN Netzen als Grundlage für eine rechtliche Beurteilung gegeben. Gleichzeitig wird abrisshaft auf die in der Literatur veröffentlichten Fehler in dem Standard eingegangen.

2.1 Anmeldung

Die Basisstation eines Wave-LAN Netzes sendet mehrmals pro Sekunde ein sogenanntes *beacon*-Signal auf dem ihr zugewiesenen Kanal. Dieses *beacon*-Signal enthält neben anderen Informationen über das Netz auch den Namen (*SSID* genannt) und die weltweit eindeutige Adresse des Netzes beziehungsweise der Basisstation. Da diese Adressen herstellerabhängig vergeben werden, lässt sich anhand der Adresse auch der Hersteller der Basisstation ermitteln. Weiterhin enthält das *beacon*-Signal unter anderem Informationen darüber, ob Verschlüsselung verwendet, welcher Kanal genutzt und welche Geschwindigkeiten unterstützt werden.

Steuernachrichten, die zwischen Basisstation und einem Computer ausgetauscht werden, sind unter anderem *probe request*, *probe response*, *authentification request* und *authentification response*. Ein Computer sendet einen *probe request* an einen bestimmten *SSID*, um Informationen über das Netzwerk zu enthalten. Darauf antwortet die Basisstation des entsprechenden Netzwerks mit einem *probe response*, der in etwa die gleichen Daten enthält, wie das *beacon*-Signal. Wenn beim *probe request* kein *SSID* angegeben wird (auch als *broadcast SSID* bezeichnet), antworten alle Basisstationen unabhängig von ihrem *SSID*.

Eine Basisstation und damit auch das zugehörige Netz können allerdings als “versteckt” konfiguriert werden; dies wird als *closed network access control*, *hidden SSID* oder *no broadcast SSID* bezeichnet. Bei dieser Einstellung, sendet die Basisstation in den *beacon*-Signalen nicht ihren *SSID* und antwortet auch nicht auf *probe request* Nachrichten an den *broadcast SSID*.

Dieser Versuch einer Zugriffsbeschränkung scheitert jedoch, da der Netzname in zahlreichen Steuerpaketen übertragen wird und somit von jedem, der in der Lage ist, Datenkommunikation zwischen der Basisstation und anderen Computern zu empfangen, ermittelt werden kann.

Bevor ein Computer mit einer Basisstation einen Nutzdatentransport vornehmen kann, muss er sich zunächst mittels eines *authentication request* bei der Basisstation authentifizieren. Bei einer *open system* Konfiguration wird praktisch keine Authentifizierung durchgeführt. *Shared Key* Authentifizierung soll nur Computern, die ein Passwort für das Netz besitzen, den Zugriff ermöglichen. Allerdings hat ein Fehler im Protokolldesign die Folge, dass jeder, der die erfolgreiche Authentifizierung eines anderen Computers bei einer Basisstation beobachtet, selbst eine solche ohne Kenntnis des Passwortes vortäuschen kann. Dazu werden praktisch nur zwei Datenpakete, die bei der erfolgreichen Authentifizierung eines anderen Rechners mitgeschnitten wurden, mathematisch verknüpft, um gültige neue Authentifizierungsdaten zu erhalten [3].

In der Regel bieten die Basisstationen eine weitere Möglichkeit zur Zugriffsbeschränkung namens *MAC-Address Control*.[1] Jede Netzwerkkarte in den Computern verfügt über eine weltweit eindeutige sogenannte *MAC*-Adresse. Der Administrator der Basisstation kann bestimmte *MAC*-Adressen vom Zugriff ausschließen oder den Zugriff auf bestimmte *MAC*-Adressen beschränken. Jedoch kann der Benutzer die *MAC*-Adresse seines Computers ändern. Er muss somit nur die Adresse seiner Netzwerkkarte softwareunterstützt auf den Wert einer berechtigten Karte ändern und erhält damit Zugriff. Welche Adressen berechtigt sind, kann entweder durch Beobachten der Kommunikation oder durch automatisiertes Ausprobieren aller möglichen Adressen eines Herstellers erfolgen.

[1] MAC: Medium Access Control.

2.2 Datentransport

Für die Nutzdaten ist ein optionaler Schutz durch Verschlüsselung vorgesehen. Der Wave-LAN-Standard definiert ein Verschlüsselungsprotokoll namens *WEP* (*Wired Equivalent Privacy*), das für drahtlose Netze die gleiche Sicherheit bieten soll, die drahtgebundene Netze von sich aus haben.

Ohne auf die technischen Details einzugehen, sollen hier einige der Angriffe auf den verschlüsselten Datentransport genannt werden:

- **Schlüssel zurückrechnen:** Durch das Mitschneiden von verschlüsselten Datenpaketen kann der verwendete Schlüssel berechnet werden. Mit diesem Schlüssel können dann sowohl sämtliche mitgeschnittene Kommunikation entschlüsselt als auch vom Angreifer Daten über das Funknetz verschickt werden [4].
- **Wörterbuch Attacke:** Durch Mitschneiden einer erheblichen Menge verschlüsselter Datenpakete können einzelne Datenpakete dekodiert werden, ohne dass der Schlüssel bekannt sein muss [3].
- **Paket Modifikation:** Bits in Datenpaketen können gekippt werden. Damit sind, soweit Struktur oder Inhalt des verschlüsselten Datenpakets zumindest teilweise bekannt sind, gezielte Modifikationen an den verschlüsselten Daten möglich ohne dass der Schlüssel bekannt sein müsste [3].
- **Paket Erstellung:** Wenn von einem Paket der verschlüsselte und unverschlüsselte Inhalt bekannt sind – wie es beispielsweise bei den *authentication request* und *authentication reply* Paketen der Fall ist –, dann kann daraus ein beliebig langes verschlüsseltes Paket erstellt werden. Das so entstandene Paket lässt sich in jedes beliebige andere, verschlüsselte und gültige Paket umwandeln [5].

- **Brute Force Attack:** Aufgrund von Fehlern in der Schlüsselerzeugung bestehen gute Chancen den Schlüssel durch Ausprobieren zu erraten. Bei den Implementierungen einiger Hersteller reichen wenige Minuten des Ausprobierens [6].
- **Replay Attack:** Es sind mehrere Angriffe veröffentlicht, die sich zu Nutze machen, dass bei *WEP* das Verschlüsseln einer bereits verschlüsselten Nachricht zu einer entschlüsselten Nachricht führt. So kann man eine verschlüsselte Nachricht aus der Luft mitschneiden und dann von außen erneut über die Basisstation in das Funknetz senden. Die Basisstation wird eine erneute Verschlüsselung versuchen, mit dem Erfolg, dass sie die Daten unverschlüsselt sendet [3].
- **Evil Twin:** Es wird eine zweite Basisstation mit gleichem Namen aber größerer Sendeleistung installiert. Die meisten Clients werden nun die zweite Basisstation nutzen. Wenn die zweite Basisstation ohne Verschlüsselung betrieben wird, schalten die Clients oftmals automatisch die Nutzung von Verschlüsselung ab. Somit erhält ein Angreifer nicht nur Zugriff auf unverschlüsselte Daten, sondern kann auch mittels einer sogenannten *Man-in-the-Middle Attack* die nun über seine Basisstation laufenden Daten beliebig verfälschen und damit ggf. weitere Sicherheitsmechanismen aushebeln [7].

3 Methodik

Um einen Überblick über die Verbreitung und Sicherheitskonfiguration von Wave-LANs zu gewinnen und eine Abschätzung des Aufwands zum Entdecken von Wave-LANs zu ermöglichen haben wir eine Messkampagne durchgeführt.

Als Testgebiet wurde das Stadtgebiet von Bonn gewählt. Zur Verifizierung und Ausweitung der in Bonn gewonnenen Ergebnisse wurden auf Kölner Gebiet stichprobenweise Messungen vorgenommen.

Für einen Pre-Test kamen handelsübliche Notebooks, Wave-LAN-Karten und ausschließlich die mitgelieferten Programme zum Einsatz. Für diesen Pre-Test wurde die Umgebung der Rechts- und Staatswissenschaftlichen Fakultät in Bonn gewählt. In der Netzwerkkonfiguration der beiden Notebooks wurde kein Netzwerk spezifiziert. Während die zu untersuchenden Straßen abgegangen wurden, musste darauf geachtet werden, ob die Konfigurationssoftware ein Netzwerk anzeigte. Wenn ja, wurde der Standort notiert, das Notebook aus dem Sendebereich des Netzes entfernt und der Netzname wieder auf unspezifiziert gesetzt.

Bei diesem Pre-Test gelang es, innerhalb einer knappen Stunde sechs Wave-LAN-Netze zu registrieren.

Für eine Untersuchung des gesamten Bonner Stadtgebietes erschien diese Methodik ungeeignet, weil sie langsam und arbeitsaufwendig ist. Es gibt jedoch auch Programme, die das Protokollieren von Netzwerkinformationen und zurücksetzen des Netzwerknamens vollautomatisch erledigen. Das am fortgeschrittenste Programm dieser Art für das Betriebssystem Microsoft Windows ist *Netstumbler*, das frei erhältlich ist. Für auf BSD 4.4lite basierende Betriebssysteme leistet *dstumbler* ähnliches.

Beide Programme führen grundsätzlich dieselben Funktionen aus, die im Pre-Test von Hand vorgenommen wurden, protokollieren jedoch zusätzlich mit Hilfe eines externen GPS Empfängers die aktuelle Position. Außerdem protokollieren sie die von Software für Endanwender in aller Regel ausgefilterten Netze mit *hidden SSID*.

Die Software stellt jeweils nur passiv die Existenz und Sicherheitskonfiguration eines Netzwerkes anhand von Steuerdaten fest und sammelt keinerlei verschlüsselte oder unverschlüsselte Nutzdaten.

Um ein ganzes Stadtgebiet zu erfassen, wurden die Messungen vom Auto aus vorgenommen. Unsere Tests ergaben, dass bei Geschwindigkeiten bis 65 km/h eine zuverlässige Erkennung von Netzwerken möglich ist. Da dieser Messaufbau von den bereits bekannten Wave-LANs nur zwei erkannte, wurde – um dem Abschirmungseffekt der Autokarosserie entgegenzuwirken – daraufhin eine handelsübliche Auto-Außenantenne mit 7db Leistung verwendet. Mit dieser Antenne konnten von den sechs bekannten Netzen vier erfasst werden.

Die Messkampagne wurde im direkten Anschluss an den Pre-Test, von Mitte Oktober bis Ende November 2001 von M. Dornseif und C. Klein durchgeführt. Um die Verkehrsbelastung möglichst gering zu halten, wurden die Messfahrten in aller Regel in den späten Abend- oder frühen Morgenstunden durchgeführt. Daher konnten nur Netze erfasst werden, die auch nachts in Betrieb waren. Während wir nicht davon ausgehen, das ein signifikanter Anteil der Basisstationen über Nacht ausgeschaltet wird, sind Ad-Hoc Netze, die nur aus Computern ohne Basisstation bestehen, vermutlich über Nacht mitsamt der sie konstituierenden Computer ausgeschaltet.

Wir haben versucht, die zentralen Stadtteile von Bonn zu erfassen. In den weiter außerhalb liegenden Stadtteilen mussten wir uns mit stichprobenhaften Messfahrten begnügen. Insgesamt wurden 20 Messfahrten mit zusammen knapp 800 km Strecke durchgeführt.

4 Messergebnisse

Auf Bonner Stadtgebiet konnten wir 157 Netze ermitteln. Da wir von den uns vorher bekannten Netzen nur 2/3 mit unserer Ausrüstung erkennen konnten, gehen wir davon aus, dass die Gesamtzahl der (auch außerhalb der üblichen Bürozeiten betriebenen) Netze in dem von uns erfassten Bonner Gebiet bei etwa 200 liegt. Bei Stichproben in Köln entdeckten wir weitere 125 Netze, die in die Gesamtauswertung mit einflossen. Von diesen insgesamt 283 Netzen waren nur 11 (ca. 4%) *Ad-Hoc* Netze. 78 Netzte (ca. 28%) nutzten *WEP* Verschlüsselung und 59 (ca. 21%) waren versteckt (*hidden SSID*).

> Das bedeutet, dass über die Hälfte der von uns entdeckten Netze die Sicherheitsfunktionen des Protokolls nicht nutzten.

Es ist bemerkenswert, dass von den Netzen, die *hidden SSID* nutzten, 58 (ca. 98%) bei demselben Netzbetreiber angesiedelt waren.

Von den 283 gefundenen Netzen hatten 84 (ca. 30%) erkennbar die von den diversen Herstellern bei der Auslieferung voreingestellten Namen. Wahrscheinlich werden Betreiber, die nicht einmal den Namen ihres Netzes ändern, auch die Sicherheitseinstellungen nicht an ihre Bedürfnisse anpassen.

5 Strafrechtliche Bewertung

Die strafrechtliche Bewertung der eingangs skizzierten, verschiedenen Angriffsmethoden auf Wave-LANs wird zur Zeit noch nicht umfassend diskutiert. Dies mag hauptsächlich daran liegen, dass Angriffe auf funkbasierte Computernetzwerke zumeist unentdeckt bleiben dürften. Gleichzeitig ist Computerkriminalität ohnehin – wie andere white collar crimes – bekannt dafür, eine hohe Dunkelziffer zu haben. In der Polizeilichen Kriminalitätsstatistik 2000 macht das Ausspähen von Daten nur knapp 1% der erfassten Computerkriminalitätsdelikte aus. In

der Rechtspraxis spielen diese Angriffe damit in der Tat eine untergeordnete Rolle.

5.1 § 202a StGB

Dem ungeladenen Gast in einem Wave-LAN bietet sich die ganze Palette der computerstrafrechtlichen Handlungsmöglichkeiten. Die einschlägigen Regelungen im StGB sind hier §§ 202a, 303a, b; wobei §§ 303a, b beim Angriffsobjekt selbst, den Daten, auf § 202a StGB verweisen. § 202a StGB bietet also das rechtliche Einfallstor bei Angriffen auf Funknetzwerke.

Diese Strafvorschrift wurde bereits mit dem 2. WiKG 1986 eingeführt und sollte Strafbarkeitslücken schließen, die mit der zunehmenden Entschriftlichtung des Informationsverkehres entstanden waren; der bisher für die Fälle der Verletzung von Privatgeheimnissen geschaffene § 202 StGB umfasst ausdrücklich lediglich Briefe und verschlossene Schriftstücke und wird somit dem heute stattfindenden Informationsaustausch über Computernetzwerke nicht gerecht. § 202a StGB schützt richtigerweise nach herrschender, jedoch nicht unbestrittener Ansicht sowohl den persönlichen Lebens- und Geheimbereich sowie ein allgemeines, durch das Erfordernis der besonderen Sicherung formalisiertes Interesse an der Geheimhaltung von Daten, die nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden [8].

Die hier relevante Tathandlung besteht nach dem Wortlaut der Vorschrift darin, dass der Täter sich oder einem anderen unbefugt Daten, die nicht für ihn bestimmt sind und die gegen unberechtigten Zugang besonders gesichert sind, verschafft.

Der Gesetzgeber hat die Tatobjekte, die Daten, im zweiten Absatz der Vorschrift legaldefiniert. Hiernach sind Daten im Sinne der Vorschrift lediglich solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Hier kommen sowohl gespeicherte und in der Übermittlung befindliche Daten in Betracht. Bei Angriffen auf ein Funknetzwerk zum aktiven oder passiven Mitlesen des Datenverkehrs greift die zweite Alternative der in der Übermittlung befindlichen Daten. Wenn das Funknetzwerk nur als Vehikel genutzt wird, um die Daten aus einzelnen Rechnern auszulesen, ist die erste Alternative einschlägig.

5.2 Ausspähen von gespeicherten Daten

Die strafnormrelevanten Angriffsobjekte beim Eindringen in ein Funknetzwerk zur Auslesung der auf den Netzrechnern gespeicherten Daten sind schnell gefunden und entsprechend definiert, wobei auch hierfür die einschränkende Voraussetzung, dass diese Daten „gegen unberechtigten Zugang besonders gesichert sind“, gegeben sein muss. Dies hängt davon ab, ob dem Eindringen in das Netzwerk Zugangssperren entgegengesetzt werden oder ob die entsprechenden Daten auf den Rechnern selbst eigene Zugangssperren aufweisen.

Solche Zugangssperren auf Wave-LAN Ebene können in *hidden SSID-, shared key- oder MAC-Adress Control*-Systemen bestehen. Wie allerdings schon oben festgestellt wurde, ist es für den einigermaßen versierten Computernutzer mit einfachen Mitteln möglich, die meisten dieser Zugangssperren zu umgehen.

Damit stellt sich insbesondere die Frage, ob diese Sicherungssysteme eine „besondere Sicherung“ im Sinne des Tatbestandes des § 202a StGB darstellen. Hierzu wird in der Literatur ein breites Spektrum an Ansichten vertreten.

Einige Literaturstimmen wollen eine besondere Sicherung nur dann annehmen, wenn diese objektiv geeignet ist, gegenüber versierten EDV-Experten eine erhebliche Hürde darzustellen [9, 10]. Nach wohl überwiegender Ansicht soll es ausreichen, wenn der versierte EDV-Anwender, oder auch der sachkundige Laie, hier auf ein erhebliches Hindernis stößt. Wobei sich hierbei noch keine klare Linie abzeichnet [11-18]. Wie oben in unserer Sachanalyse dargelegt, ist es bis in die Laienebene hinunter mit einfachen Mitteln möglich, Zugriff auf die Netzwerke zu erhalten. Im Hinblick auf Funknetzwerke existieren in der Praxis noch keine entsprechend anspruchsvollen und gleichzeitig praxistauglichen Sicherungen. Es sollte deshalb reichen, hier an dem interessierten Laien anzusetzen. Dieser muss sich, sieht er sich den gängigen Zugangssperren gegenüber, schon intensiv mit dem Netzwerk auseinandersetzen, eventuell Passworte errechnen oder seine Adressdaten modifizieren.

Mit den in Rede stehenden Arten der Zugangssperren dürfte also der Netzwerkbetreiber sein Geheimhaltungsinteresse gegenüber den meisten Angreifern genügend dokumentieren. Soweit er dies getan hat, ist er gegen Abruf von Daten von seinen Rechnern strafrechtlich geschützt.

5.3 Ausspähen von in der Übertragung befindlichen Daten

Hinsichtlich der Attacken auf die Übertragungsdaten, also die Daten, die Gegenstand des Funkverkehres selbst sind, bietet sich ein ähnliches Bild. Hierzu muss bei der Frage nach der Strafbarkeit des Angriffs auf das Funknetzwerk zunächst in jedem Falle geklärt werden, ob der Netzwerkbetreiber die Datenübertragung physisch, z.B. durch Abschirmungsmaßnahmen, gesichert hat. Ist dies der Fall, ist in der Regel von einer besonderen Sicherung im Sinne des Tatbestandes auszugehen, die Übertragungsdaten sind damit strafrechtlich geschützt.

Existieren keine gesonderten physischen Sicherungsmaßnahmen ist zu klären, ob der Betreiber die Option der Datenverschlüsselung (*WEP*) wahrgenommen hat. Ist dies nicht der Fall, so scheidet eine Strafbarkeit nach § 202a StGB für den Angreifer grundsätzlich aus, da die Übertragungsdaten damit regelmäßig nicht gesichert sind.

5.4 Rechtliche Wertung der Verschlüsselung

Es stellt sich mit Blick auf den Wortlaut des § 202a StGB dann allerdings die Frage, ob wir es bei Verschlüsselungen mit „besonderen Zugangssicherungen“ zu tun haben, eine Frage, die in Wissenschaft und Rechtsprechung noch nicht abschließend geklärt worden ist.

Der Gesetzgeber hat mit der Schaffung des § 202a StGB gerade auch Daten schützen wollen, die sich im Übertragungsstadium befinden. Hierzu sollte es egal sein, ob die Datenübertragung über Kabel oder Funk vonstatten geht [19].

Nutzt der Betreiber allerdings eine Verschlüsselung, so ist zu bemerken, dass die verschlüsselten Daten selbst *offen*, also ohne weiteren Schutz übertragen werden. Der Wortlaut des § 202a StGB, spricht jedoch von Daten, die gegen unberechtigten Zugang besonders gesichert sind. Die Verschlüsselung selbst stellt aber nur neue Daten her, die selbst der Übertragung unterliegen. Die Originaldaten, die Gegenstand der Verschlüsselung sind, existieren in ihrem Urzustand zwar weiter, jedoch unabhängig von den nun eigenständig versendeten Ü-

bertragungsdaten. Ziel der möglichen Attacken auf das Funknetz sind aber gerade diese (verschlüsselten) Daten. Gegenstand der Regelung des § 202a StGB sind alle Daten, die dem Interesse an der Geheimhaltung unterliegen. Ob nun eine Klartextnachricht oder ein auf den ersten Blick unauflösbarer „Datensalat“ (in Form der verschlüsselten Daten) Ziel des Angriffs ist, spielt damit für die Strafbarkeit keine Rolle.

Objekt unserer Betrachtung müssen also die verschlüsselten Daten sein und nicht irgendwie dahinterstehende Prototypen, die Originaldaten. Fassen wir nun allerdings richtigerweise die hier relevanten Übertragungsdaten als unabhängige Daten auf, so ist festzustellen, dass hier lediglich völlig ungeschützte Daten geradezu „aus der Luft gegriffen“ werden können.

In der strafrechtlichen Literatur zu § 202a StGB werden häufig Verschlüsselungen trotzdem als besondere Sicherungen angesehen [8, 15, 16, 20]. Zum Teil wird hier festgestellt, dass die Kenntnisnahme der verschlüsselten Daten nicht mehr als Zugang zu den Originaldaten angesehen werden kann [16]. Dies ist zwar richtig, spielt aber in unserer Betrachtung keine Rolle, weil Angriffsobjekt eben nur die konkreten verschlüsselten Daten sind.

Weiterhin wird in der Literatur nach dem Sinn und Zweck der Norm argumentiert. Die Zugangssicherung im Sinne des Tatbestandes diene dem Zweck, das formalisierte Interesse an der Geheimhaltung zu schützen. Im Falle der Datenübertragung könne dieser Zweck eben nur durch Verschlüsselung erreicht werden. Das Gesetz sei daher entsprechend auszulegen, dass auch Verschlüsselungen als besondere Sicherung im Sinne des Tatbestandes verstanden werden müssten [16]. Mit ähnlichen Argumentationen kommen auch andere Literaturstimmen zu diesem Ergebnis. Sie haben allerdings gemeinsam, soweit sie diesen Punkt überhaupt problematisieren, dass sie hier vornehmlich noch immer auf die Originaldaten eingehen und den verschlüsselten Daten keine eigene Tatobjektsqualität zuweisen.

Nur vereinzelt wird eine besondere Sicherung im Sinne des § 202a StGB bei der Übertragung von verschlüsselten Daten abgelehnt [21]. Unter Berücksichtigung der auch hier vertretenen Ansicht, dass eine einheitliche Betrachtung von Originaldaten und verschlüsselten Daten nicht angebracht ist, ist dieser Ansicht im Ergebnis zuzustimmen.

> Es zeigt sich somit bei richtiger dogmatischer Bewertung des § 202a StGB, dass verschlüsselte Daten regelmäßig keinen strafrechtlichen Schutz genießen.

Es bleibt abzuwarten, in welche Richtung die künftige Rechtsprechung bei Angriffen auf Funknetzwerke geht. Es steht zu befürchten, dass die Gerichte hier der herrschenden Ansicht folgen und auch das Aufgreifen von verschlüsselten Daten dem § 202a StGB unterstellen. Dies müsste sich dann aber auf eher an dem Ergebnis orientierten Überlegungen stützen, da nach richtiger Betrachtung des Wortlautes des § 202a StGB hier unangenehme Strafbarkeitslücken zu verzeichnen sind.

6 Fazit

Wir haben gezeigt, dass es unmöglich ist, mit den heute auf dem Massenmarkt erhältlichen Systemen ein vollständig angriffssicheres Wave-LAN zu betreiben.

Wir haben weiterhin gezeigt, dass Wave-LANs eine nicht unbedeutende Verbreitung haben und anscheinend überwiegend ohne Verschlüsselung und andere Sicherheitsmechanismen betrieben werden.

Schließlich wurde dargelegt, dass der Betreiber eines ungeschützten Wave-LANs praktisch keinerlei strafrechtlichen Schutz vor Ausspähen seiner Daten erwarten kann und nur sehr unvollständigen Schutz vor aktiven Angriffen auf sein Netz hat.

Selbst bei verschlüsselt betriebenen Netzwerken ist die strafrechtliche Situation beim Ausspähen dogmatisch höchst unbefriedigend. Gegen aktive Angriffe hingegen bietet das Strafrecht grundsätzlich Schutz, soweit ein Geheimhaltungsinteresse dokumentiert wird. Diese Dokumentationsfunktion kann jeder der Wave-LAN-Sicherheitsmechanismen erfüllen.

Da hinreichend publiziert wurde, dass Wave-LANs unsicher sind, muss der Nutzer eines Wave-LANs damit rechnen, selbst einen Schuldvorwurf gemacht zu bekommen, wenn Daten über ein Wave-LAN in falsche Hände gelangen.

> Unter dem Strich ist jedem Nutzer von Wave-LANs, der darüber schutzwürdige Daten überträgt, zu raten, sich ernsthaft zu fragen, ob er nicht dem Beispiel des *Lawrence Livermore National Laboratory* folgt und die Wave-LAN-Nutzung aus Sicherheitsgründen ganz unterlässt.

Literatur

[1] Eine umfangreiche Sammlung mit Web-Verweisen zum Thema WaveLAN findet sich unter http://md.hudora.de/comp/krim/Rechtstatsachenforschung/WaveLAN/

[2] R. Weiss, S. Lucks: *Standardmäßige Wave-LAN Unsicherheit* , DuD 2001, S. 665ff

[3] N. Borisov, I. Goldberg, D. Wagner: *Intercepting Mobile Communications,* http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

[4] A. Stubbefield, J. Joannidid, A.D. Rubin: *Using the Fluhrer, Mantin and Shamir Attack to break WEP*, AT&T Labs TR TD-4ZCPZZ, 21. August 2001 http://www.cs.rice.edu/~astubbe/wep/

[5] W. A. Arbaugh *An Inductive Chosen Plaintext Attack Against WEP/WEP2*, http://www.cs.umd.edu/~waa/attack/v3dcmnt.htm

[6] T. Newsham: *Cracking WEP Keys,* July 2001, http://www.lava.net/~newsham/wlan/WEP_password_cracker.ppt

[7] ISS Whitepaper: *Wireless LAN Security,* http://documents.iss.net/whitepapers/wireless_LAN_security.pdf

[8] Lackner/Kühl, § 202a StGB.

[9] Leicht, iur 1987. S. 45 ff.

[10] Jessen*, Zugangsberechtigung und besondere Sicherung iSd § 202a StGB*, S. 119 ff.

[11] LK-Jähnke, § 202a.

[12] Granderath, 2. WiKG, DB 1986 Beilage 18, Seite 1.

[13] Möhrenschlager, wistra 1986, Seite 140.

[14] Weber, WM 1986, Seite 1133 ff.

[15] Tröndle/Fischer-Fischer, § 202a Rn. 7a.

[16] Lenckner/Winkelbauer, CR 1986, Seite 485ff.

[17] Hilgendorf, JuS 1996, Seite 702.

[18] Sch/Sch-Lenckner, § 202a.

[19] BT-Drs. 10/5058, Seite 29.

[20] Schulze-Heiming, *Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls*, Seite 75 f.

[21] P. Schmid, *Computerhacken und materielles Strafrecht*, Seite 103f.