Eine empirische Untersuchung zur Verbreitung und Sicherheit von WLAN-Infrastrukturen

Daniel Fischer, Dirk Stelzer

Institut für Wirtschaftsinformatik
Fachgebiet Informations- und Wissensmanagement
Technische Universität Ilmenau
Postfach 100565
98684 Ilmenau
{daniel.fischer | dirk.stelzer}@tu-ilmenau.de

Abstract: Der Beitrag fasst wesentliche Ergebnisse einer empirischen Untersuchung zur Verbreitung und Sicherheit von Wireless LAN-Infrastrukturen (WLAN) in deutschen Unternehmen und Behörden zusammen. Die Untersuchung mit explorativem Charakter wurde von November 2005 bis Januar 2006 durchgeführt. Es werden Erkenntnisse über die Verbreitung der WLAN-Technologie, den Einsatz von Sicherheitsmaßnahmen und die Zusammenhänge zwischen unternehmensspezifischen Merkmalen und dem Einsatz von Sicherheitsmaßnahmen in WLAN-Infrastrukturen ermittelt.

1 Einführung

Die Bedeutung funkbasierter Netze, so genannter Wireless Local Area Networks (WLAN)[1], hat in den vergangenen Jahren stark zugenommen [BSI03a, De03]. Die durch WLAN ermöglichte Mobilität und Flexibilität ist jedoch oft mit großen Sicherheitsdefiziten verbunden [BG03, RSA05, SL04]. So zeigt beispielsweise eine Untersuchung von RSA-Security, dass in London, New York, San Francisco und Frankfurt über ein Drittel aller WLAN-Infrastrukturen von Unternehmen völlig ungesichert ist [RSA05]. Obwohl viele Sicherheitsmaßnahmen[2] für WLAN-Infrastrukturen verfügbar sind, werden diese offenbar nicht oder nicht angemessen eingesetzt. Bisherige Untersuchungen, welche die Einsatzhäufigkeit von WLAN-Sicherheitsmaßnahmen sowie Gründe für deren Nichteinsatz analysierten, beschränken sich meist nur auf einzelne Sicherheitsmaßnahmen [BG03, RSA05]. Außerdem fehlen Analysen, die Zusammenhänge zwischen unternehmensspezifischen Merkmalen und dem Einsatz von WLAN-Sicherheitsmaßnahmen untersuchen.

[1] In dieser Arbeit betrachten wir ausschließlich Funknetze der IEEE 802.11-Protokollfamilie.

[2] Unter einer Sicherheitsmaßnahme verstehen wir jede Maßnahme, die zur Erhöhung der Sicherheit in einem System - hier: in einer WLAN-Infrastruktur - führen kann [St93]. Sicherheitsmaßnahmen wirken gegen ein oder mehrere Schwachstellen und verhindern, dass sicherheitsgefährdende Ereignisse eintreten oder reduzieren das damit verbundene Schadenspotential.

In diesem Beitrag beschreiben wir wesentliche Ergebnisse einer explorativen Untersuchung zur Verbreitung und Sicherheit von WLAN-Infrastrukturen in deutschen Unternehmen und Behörden [FSK06]. Insbesondere werden folgende Fragen diskutiert:

- Wie verbreitet sind WLAN-Infrastrukturen?
- Wie häufig kommen welche Sicherheitsmaßnahmen zum Einsatz?
- Warum werden einige Sicherheitsmaßnahmen eingesetzt, andere jedoch nicht?
- Welche Zusammenhänge gibt es zwischen unternehmensspezifischen Merkmalen und dem Einsatz einzelner Sicherheitsmaßnahmen?

Im folgenden Abschnitt wird auf die Vorbereitung und Durchführung der Untersuchung eingegangen. Im dritten Abschnitt dokumentieren und diskutieren wir die zentralen Ergebnisse. Im letzten Abschnitt nehmen wir eine kritische Würdigung unserer Erkenntnisse vor und geben einen Ausblick auf weitere Forschungsaufgaben.

2 Aufbau und Durchführung der Untersuchung

Zur Konkretisierung der in der Einleitung gestellten Fragen entwickelten wir Hypothesen über die Verbreitung der WLAN-Technologie, den Einsatz von WLAN-Sicherheitsmaßnahmen und die Gründe des Nichteinsatzes sowie über Zusammenhänge zwischen unternehmensspezifischen Merkmalen und dem Einsatz von Sicherheitsmaßnahmen.[3] Unter Verwendung von Methoden der deskriptiven Statistik sollen diese Hypothesen im Rahmen der Untersuchung diskutiert werden [Sa04a].

Bei der Auswahl der Untersuchungsform entschieden wir uns für eine Internet-basierte Befragung (Online-Befragung) [Kr02]. Sie ist im Vergleich zu anderen Erhebungsmethoden mit geringerem zeitlichen und finanziellen Aufwand durchführbar. Für die Befragung entwickelten wir einen Fragebogen[4], der sich in drei Teile gliedert. Im ersten Teil werden Informationen über die befragten Institutionen sowie ihr IT-Sicherheitsmanagement ermittelt. Der zweite Teil enthält Fragen zu den WLAN-Infrastrukturen. Im letzten Teil werden die Befragungsteilnehmer nach Sicherheitsmaßnahmen befragt. Grundlage dieses Fragebogenteils ist unser Katalog WLAN-spezifischer Sicherheitsmaßnahmen[5]. Er enthält 46 Sicherheitsmaßnahmen, die den Klassen a) organisatorische Maßnahmen vor der Inbetriebnahme, b) organisatorische Maßnahmen während des Betriebs, c) hardware-technische Maßnahmen und d) software-technische Maßnahmen zugeordnet sind.[6] Für jede Sicherheitsmaßnahme wird ermittelt, ob sie dem Befragungsteilnehmer bekannt ist und ob sie eingesetzt wird. Für den Fall, dass eine bekannte Sicherheitsmaßnahme nicht eingesetzt wird, fragten wir nach dem Grund dafür.

---

[3] Für die Hypothesenbildung analysierten wir Fachliteratur [BSI03c, BG03, Dete03, RSA05, Sa04b, SL04, Wi04] und die Standardspezifikationen der IEEE-802.11-Familie [IEEE06].

[4] Der Fragebogen steht unter http://www.wlan-sec.de/Fragebogen.pdf zur Verfügung.

[5] Der Maßnahmenkatalog steht unter http://www.wlan-sec.de/Massnahmenkatalog.pdf zur Verfügung.

[6] Für die Entwicklung des Maßnahmenkataloges werteten wir neben den bereits bei der Hypothesenbildung genannten Quellen die Standards ISO/IEC 17799:2005 [ISO05a] und ISO/IEC 27001:2005 [ISO05b] sowie weitere Dokumentationen, Rahmenwerke und Publikationen, wie z. B. [BSI05, FMS01, Ko04] aus.

Die Befragung führten wir im Zeitraum von November 2005 bis Januar 2006 in Kooperation mit dem IT-Dienstleister NetSys.IT Information & Communication, dem TeleTrusT Deutschland e.V., dem Wirtschafts- und Innovationsportal Thüringen (WIP) und dem Wirtschaftsnetz Thüringen (WNT)[7] durch. Bei der Auswahl der Stichprobe konzentrierten wir uns auf die Mitglieder unserer Kooperationspartner TeleTrusT und WIP.[8] Insgesamt verschickten wir an 1.164 Unternehmen und Behörden via E-Mail Einladungen zur Teilnahme.

3 Beschreibung und Analyse der Ergebnisse

Von den 1.164 eingeladenen Unternehmen und Behörden nahmen 290 an der Untersuchung teil. Dies entspricht einer Rücklaufquote von 25%. 75 der 290 Befragungsteilnehmer betreiben WLAN-Infrastrukturen. Dies ergibt eine WLAN-Verbreitung von 26%. Von den Befragungsteilnehmern mit WLAN beantworteten 36 den Fragebogenteil zum Einsatz von WLAN-Sicherheitsmaßnahmen vollständig. Unser Analysedesign beschränkt sich auf die Ermittlung von Häufigkeiten, Mittelwerten und Varianzen. Mit Hilfe dieser Kenngrößen diskutieren wir im Folgenden die aufgestellten Hypothesen. Auf Signifikanztests haben wir verzichtet, da die Stichprobe nicht zufällig erhoben wurde und die Anzahl vollständig ausgefüllter Fragebögen relativ gering ist.

3.1 Verbreitung von WLAN-Infrastrukturen

Hypothese 1: Der Betrieb von WLAN-Infrastrukturen in Unternehmen und Behörden hat im Vergleich zu vergangenen Jahren stark zugenommen. Zur Untersuchung dieser Hypothese erfragten wir, ob und seit wann WLAN-Infrastrukturen eingesetzt werden. Die Analyse der Einsatzjahre ergab, dass seit 2002 eine stetige Zunahme der Verbreitung zu beobachten ist. Dieser Trend wird auch 2006 fortgesetzt, da bereits 20 Befragungsteilnehmer die Inbetriebnahme von WLAN-Infrastrukturen für dieses Jahr planten. Dies spricht für eine Bestätigung der Hypothese 1.

Hypothese 2: Hauptsächlich große Unternehmen und Behörden mit einem entsprechenden IT-Know-how setzen WLAN-Infrastrukturen ein. Wir nahmen an, dass größere Institutionen im Vergleich zu kleineren über ein umfangreicheres IT-Know-how verfügen und aus diesem Grund häufiger WLAN-Infrastrukturen einsetzen. Unsere ermittelten Ergebnisse unterstützen diese Hypothese, da 38% der Institutionen mit über 250 Mitarbeitern und 32% der Institutionen mit 51 bis 250 Mitarbeitern WLAN-Infrastrukturen einsetzen. Dagegen betreiben nur 15% der kleinen Institutionen mit 10 bis 50 Mitarbeitern sowie 29% der Kleinstinstitutionen mit weniger als 10 Mitarbeitern WLAN-Infrastrukturen. Interessant ist, dass insbesondere kleinere und mittlere Institutionen in naher Zukunft den Einsatz von WLAN-Infrastrukturen planen.

---

[7] Weitere Informationen zu den Kooperationspartnern unter http://www.netsys-it.de, http://www.teletrust.de, http://www.wip-thueringen.de und http://www.wn-thueringen.de.

[8] Mitglieder des TeleTrusT e.V. sind Unternehmen und Behörden aus ganz Deutschland, die gemeinsam die Vertrauenswürdigkeit von Informations- und Kommunikationstechnik fördern. Mitglieder des WIP sind Unternehmen und Behörden, die in Thüringen tätig sind.

3.2 Einsatz von WLAN-Sicherheitsmaßnahmen sowie Gründe für den Nichteinsatz

Hypothese 3: Unternehmen und Behörden setzen mehr technische als organisatorische Sicherheitsmaßnahmen ein. WLAN-Infrastrukturen sind sowohl durch technische als auch durch organisatorische Sicherheitsmaßnahmen zu schützen. Da organisatorische Veränderungen im Vergleich zu technischen oft mit höheren Aufwänden verbunden sind, vermuteten wir einen stärkeren Einsatz technischer Sicherheitsmaßnahmen. Bei der Auswertung der durch die Befragungsteilnehmer eingesetzten Sicherheitsmaßnahmen ermittelten wir jedoch, dass mehr organisatorische (54%) als technische Sicherheitsmaßnahmen (36%) verwendet werden. Dies spricht klar gegen unsere Hypothese 3.

Maßnahme/Beschreibung	Klasse	Einsatz-häufigkeit
Werkseitige Grundeinstellungen an WLAN-Geräten ändern	Techn. Maßnahme	83 %
Eigenen Netzwerknamen vergeben (kryptische SSID)	Techn. Maßnahme	69 %
Umgebungsfaktoren beachten (Störquellen, bauliche Gegebenheiten)	Org. Maßnahmen	69 %
Administration der Access Points nicht über WLAN-Schnittstelle vollziehen	Org. Maßnahme	67 %
Zugangspasswörter von WLAN und LAN unabhängig voneinander festlegen	Org. Maßnahme	67 %
Notwendigkeit, Ziele und Anwendungszweck der WLAN-Infrastruktur begründen	Org. Maßnahme	67 %
Geeignete WLAN-Geräte (Signaltechnik: z. B. OFDM/ DSSS) und Standard (IEEE 802.11g, etc.) wählen	Techn. Maßnahme	64 %
Physischer Zugriff zu Access Points nur autorisiertem Personal ermöglichen	Org. Maßnahmen	61 %

Tabelle 1: Top-8-Liste der eingesetzten WLAN-Sicherheitsmaßnahmen

Hypothese 4: Unkenntnis und hoher Implementierungs-/Betriebsaufwand sind die Hauptgründe für den Nichteinsatz von Sicherheitsmaßnahmen. Ratgeber bzw. Beiträge zur WLAN-Sicherheit konzentrieren sich häufig auf wenige ausgewählte Sicherheitsmaßnahmen [BSI03b, Ko04]. Auch ist eine Fokussierung auf technische Aspekte zu beobachten. Dies führt zu der Annahme, dass viele WLAN-Betreiber bestimmte Sicherheitsmaßnahmen nicht kennen und demzufolge auch nicht einsetzen [BG03]. Als weiteren wichtigen Grund für den Nichteinsatz von Sicherheitsmaßnahmen vermuteten wir zu hohe Implementierungs-/Betriebsaufwände. Unsere Untersuchung ergab, dass die Befragungsteilnehmer im Durchschnitt nur 57% der im Fragebogen genannten Sicherheitsmaßnahmen kennen, 43% der Sicherheitsmaßnahmen sind ihnen unbekannt. Von den bekannten Sicherheitsmaßnahmen setzen die Befragungsteilnehmer jedoch nur 78% ein, 22% bleiben bewusst ungenutzt. Insbesondere bei den technischen Sicherheitsmaßnahmen liegen die Einsatzhäufigkeiten weit unter den Bekanntheitsgraden. Ein Beispiel hierfür sind die Authentifizierungsverfahren (Abbildung 1): Authentifizierung nach IEEE 802.1x über einen RADIUS-Server führen nur 17% der Befragungsteilnehmer durch, obwohl 53% die Sicherheitsmaßnahme kennen. Es gibt demzufolge neben der Unkenntnis noch weitere Gründe für den Nichteinsatz von Sicherheitsmaßnahmen. Als häufigster Grund (23% aller Begründungen) gaben die Befragungsteilnehmer an, dass die jeweilige Sicherheitsmaßnahme in ihren WLAN-Infrastrukturen nicht praktikabel nutzbar ist. Nur 10% begründeten den Nichteinsatz mit zu hohen Implementierungs-/ Betriebsaufwänden und weitere 8% mit einer zu geringen Wirkung der Sicherheitsmaß-

nahme. Damit können wir Hypothese 4 nur in Bezug auf die Unkenntnis von Sicherheitsmaßnahmen bestätigen. In einem weiteren Schritt analysierten wir die Begründungen des Nichteinsatzes bei einzelnen Sicherheitsmaßnahmen. Hierbei stellten wir fest, dass bei den regelmäßig durchzuführenden organisatorischen Sicherheitsmaßnahmen der hohe Implementierungs-/Betriebsaufwand der Hauptgrund für den Nichteinsatz ist.

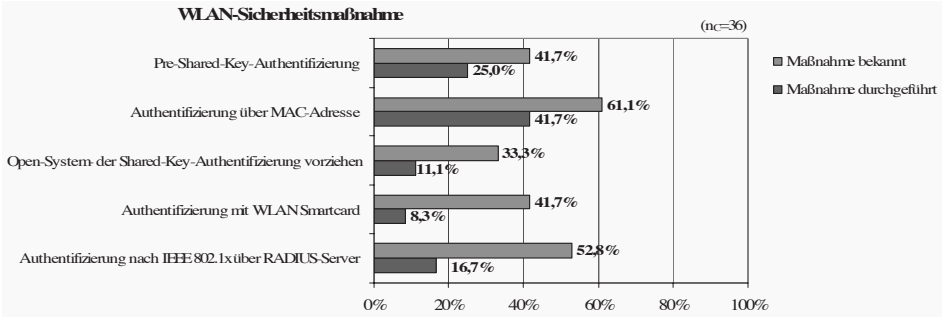

Abbildung 1: Bekanntheitsgrade und Einsatzhäufigkeiten von Authentifizierungsverfahren

3.3 Zusammenhänge zwischen unternehmensspezifischen Merkmalen und WLAN-Sicherheitsmaßnahmen

Hypothese 5: Unternehmen aus der Informations- und Kommunikationstechnik(IuK)-Branche setzen im Vergleich zu Unternehmen aus anderen Branchen und Behörden mehr Sicherheitsmaßnahmen ein. Wir gehen davon aus, dass Unternehmen aus der IuK-Branche im Vergleich zu Unternehmen anderer Branchen und Behörden über ein umfangreicheres IT-Know-how verfügen. Aufgrund dessen vermuteten wir in der IuK-Branche einen häufigeren Einsatz von Sicherheitsmaßnahmen. Für diese Hypothese spricht, dass IuK-Unternehmen im Durchschnitt 55% der im Fragebogen enthaltenen Sicherheitsmaßnahmen einsetzen. Dies ist im Vergleich zu Unternehmen anderer Branchen (Dienstleistungen: 47%; Industrie: 38%) ein deutlich höherer Wert. Die mit 25% geringste Einsatzhäufigkeit von Sicherheitsmaßnahmen ermittelten wir bei Behörden. Darüber hinaus beobachteten wir in der IuK-Branche ebenfalls einen wesentlich intensiveren Einsatz stärkerer Verschlüsselungsverfahren (WPA/WPA2). Auch hier haben Unternehmen anderer Branchen und Behörden, die eher kein oder WEP als Verschlüsselungsverfahren verwenden, großen Nachholbedarf.

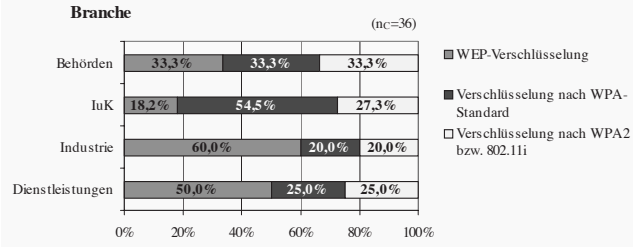

Abbildung 2: Einsatzhäufigkeiten von Verschlüsselungsverfahren in Abhängigkeit von der Branche

Hypothese 6: In Unternehmen und Behörden, die ein IT-Security-Management besitzen, ist der Einsatz von Sicherheitsmaßnahmen wesentlich höher als in Institutionen ohne IT-Security-Management. Ein IT-Security-Management dient der koordinierten Planung, Realisierung und Kontrolle der Sicherheit aller IT-Systeme. Von den 36 Befragungsteilnehmern, welche die Fragen zu den Sicherheitsmaßnahmen vollständig beantwortet haben, besitzen 25 ein IT-Security-Management (70%). Wir gingen davon aus, dass diese Unternehmen und Behörden mehr Sicherheitsmaßnahmen einsetzen als Institutionen ohne IT-Security-Management. Unsere Analyse zeigt, dass die Institutionen mit IT-Security-Management durchschnittlich 51% der im Fragebogen aufgeführten Sicherheitsmaßnahmen einsetzen. Dagegen sind es bei Institutionen ohne IT-Security-Management lediglich 25%. Dieses Ergebnis ist konform zu Hypothese 6. Einen besonders starken Zusammenhang ermittelten wir zwischen dem Vorhandensein des IT-Security-Managements und dem Einsatz organisatorischer Sicherheitsmaßnahmen.

Hypothese 7: Größere Unternehmen und Behörden setzen im Vergleich zu kleineren mehr Sicherheitsmaßnahmen in ihren WLAN-Infrastrukturen ein. Größere Institutionen besitzen meist eine oder mehrere IT-Abteilung(en) und in Folge dessen im Vergleich zu kleineren Unternehmen umfangreichere IT-Kenntnisse. Aus diesem Grund erwarteten wir, dass die Bekanntheitsgrade und Einsatzhäufigkeiten der WLAN-Sicherheitsmaßnahmen bei größeren Institutionen höher sind. Unsere Untersuchung ergab jedoch ein anderes Bild. Bei den Bekanntheitsgraden erzielen zwar die größeren Institutionen mit durchschnittlich 61% der Sicherheitsmaßnahmen das bessere Ergebnis, jedoch sind die Unterschiede zu den kleineren mit 52% relativ gering. Bei den Einsatzhäufigkeiten liegen die kleineren Institutionen mit durchschnittlich 47% sogar vor den größeren mit 39%. Dies spricht gegen Hypothese 7. Bei der Analyse der Einsatzhäufigkeiten einzelner Sicherheitsmaßnahmen konnten wir jedoch sowohl bei einigen organisatorischen als auch bei technischen Maßnahmen signifikante Abhängigkeiten von der Größe der Institution ermitteln.

4 Fazit und Ausblick

Die von uns ermittelten Ergebnisse geben erste konkrete Hinweise über die Bekanntheitsgrade und Einsatzhäufigkeiten von WLAN-Sicherheitsmaßnahmen in deutschen Unternehmen und Behörden. Darüber hinaus konnten wir erste Zusammenhänge zwischen unternehmensspezifischen Merkmalen und einzelnen WLAN-Sicherheitsmaßnahmen beobachten. Aufgrund der von uns gewählten Stichprobe (keine zufällige Auswahl) sowie der geringen Anzahl vollständig ausgefüllter Fragebögen lassen sich jedoch diese Ergebnisse nicht verallgemeinern. Problematisch ist auch, dass die Aussagen zur WLAN-Sicherheit ausschließlich auf der Anzahl eingesetzter WLAN-Sicherheitsmaßnahmen beruhen. Eine Berücksichtigung unterschiedlicher Wirkungsgrade von Sicherheitsmaßnahmen findet nicht statt. Mit dem Ziel, allgemeingültige Aussagen zu erhalten, planen wir, die Untersuchung mit einer größeren Anzahl zufällig ausgewählter Unternehmen und Behörden zu wiederholen. Dies erfordert dann auch eine Neugestaltung des Analysedesign unter Verwendung von Methoden der induktiven Statistik (z. B. Signifikanztests). Des Weiteren werden wir unseren Katalog WLAN-spezifischer Sicherheitsmaßnahmen überarbeiten. Insbesondere soll eine Bewertung der Qualität bzw. Wirkung

der Sicherheitsmaßnahmen erfolgen. Dies würde uns noch konkretere Aussagen zur Sicherheit in WLAN-Infrastrukturen ermöglichen.

Literaturverzeichnis

[BSI03a] BSI (Hrsg.): Kommunikations- und Informationstechnik 2010+3: Neue Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. http://www.bsi.de/literat/studien/trend2010/netze_kommunikation.pdf, 2003, Abruf: 2006-05-30.

[BSI03b] BSI (Hrsg.): Sicherheit im Funk-LAN (WLAN, IEEE 802.11). http://www.bsi.bund.de/literat/doc/wlan/wlan.pdf, Bonn, 2003, Abruf: 2006-05-30.

[BSI05] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Technische Richtlinie Sicheres WLAN (TR-S-WLAN). Bonn, 2005.

[BG03] Büttner, H.-G.; Gödde, D.: Wireless LAN – Studie zur Sicherheit von drahtlosen Netzwerken in deutschen Firmen. Ernst & Young IT-Security, http://www.ey.com/global/download.nsf/Germany/WLAN_Studie/$file/WLAN.pdf, 2003, Abruf: 2006-05-30.

[De03] Detecon (Hrsg.): Trendletter Public WLAN – Hot Spot Report, http://www.detecon.com/de/publikationen/studienbuecher_detail.php?pub_id=75, 12/2003, Abruf: 2006-05-30.

[FSK06] Fischer, D; Stelzer, D.; Kreyßel, D: Verbreitung und Sicherheit von Wireless LAN-Infrastrukturen – eine empirische Untersuchung unter deutschen Unternehmen und Behörden. Ilmenauer Beiträge zur Wirtschaftsinformatik Nr. 2006-03. Ilmenau 2006.

[FMS01] Fluhrer, S.; Mantin, I.; Shamir, A.: Weaknesses in the Key Scheduling Algorithm of RC4. In: Lecture Notes in Computer Science Vol. 2259 (2001), p. 1-24.

[IEEE06] IEEE: Wireless LANs Standards (802.11) – Get IEEE 802, Documentation Homepage. http://standards.ieee.org/getieee802, 2006, Abruf: 2006-06-15.

[ISO05a] ISO (Hrsg.): ISO/IEC 27001:2005: Information technology, Security techniques, Code of practice for information security management. http://www.iso.org, 2005, Abruf: 2006-05-25.

[ISO05b] ISO (Hrsg.): ISO/IEC 27001:2005: Information technology, Security techniques, Information security management systems - Requirements. http://www.iso.org, 2005, Abruf: 2006-05-25.

[Ko04] Kopp, H.: Einsatz von WLAN in Unternehmen – Leitfaden. Electronic Commerce Center Mecklenburg-Vorpommern (Hrsg.), http://www.mittelstand-sicher-im-internet.de/content-details.php?118, 9/2004, Abruf: 2006-05-30.

[Kr02] Kromrey, H.: Empirische Sozialforschung: Modelle und Methoden der standardisierten Datenerhebung und Datenauswertung. 10. Aufl., Leske&Budrich Verlag, Opladen, 2002.

[RSA05] RSA-Security (Hrsg.): The Wireless Security Survey of San Francisco. http://www.securitymanagement.com/library/rsa_wireless0606.pdf, 03/2005, Abruf: 2006-05-30.

[Sa04a] Sachs, L.: Angewandte Statistik - Anwendung statistischer Methoden. 11. Aufl., Springer, Berlin u.a., 2004.

[Sa04b] Sautner, F.: IT-Security-Studie 2004. InformationWeek. http://www.iw-live.de/security/media/it_security_2004_studieninfo.pdf, 2004, Abruf: 2005-05-30.

[SL04] Stanossek, G.; Lenz-Hawliczek, J.: WLAN-Studie Berlin. http://www.berlin.de/senwiarbfrau/projektzukunft/mat/studien/studie_wlan_2004.pdf, 08/2004, Abruf: 2005-10-10.

[St93] Stelzer, D.: Sicherheitsstrategien in der Informationsverarbeitung - Ein wissensbasiertes, objektorientiertes Beratungssystem für die Risikoanalyse. Dt. Universitätsverlag, Wiesbaden, 1993.

[Wi04] Wick Hill (Hrsg.): Wireless Networking in Deutschland. http://www.nexthop.de/de/clients/wickhill/press/wh20040915.pdf, 10/2004, Abruf: 2006-05-30.