Universität Ulm
Sektion Angewandte Informationsverarbeitung

IT-Sicherheit, Unternehmenskulturen und wirtschaftsbedrohende Kriminalität

Diplomarbeit
im Studiengang Wirtschaftsmathematik

vorgelegt von

Sven Übelacker

1. Gutachter: Professor Dr. Franz Schweiggert
2. Gutachter: Professor Dr. Dieter Beschorner

vorgelegt am 19. September 2002
aktualisierte Version vom 11. Juli 2013

Kontakt & Lizenz

Kontakt:	Sven Übelacker <sven@uebelacker.net>
Lizenz:	Creative Commons License Attribution-Share Alike 3.0 Germany
Version:	2013-07-11
Originalversion:	2002-09-19

i http://creativecommons.org/licenses/by-sa/3.0/de/

Erklärung

Hiermit erkläre ich, dass ich die Diplomarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

Ulm, den 19.09.2002 Sven Übelacker

Matrikelnummer: 411678

Danksagung

Bedanken möchte ich mich bei Prof. Franz Schweiggert für seine Unterstützung und Hilfestellung, meine Diplomarbeit durchzuführen.

Diese Diplomarbeit wäre nicht möglich gewesen, ohne die Förderung durch die Heinrich Böll Stiftung Berlin; insbesondere bedanke ich mich bei Gabriele Tellenbach vom Studienwerk für die sehr gute Betreuung während meines Studiums.

Ferner bin ich Francisco Uzcanga (Spanisch) und Heather Burton (Englisch) vom Sprachenzentrum der Universität Ulm für Übersetzungshilfe und Prof. Otto-Peter Obermeier (Gerling Akademie für Risikoforschung Zürich), der mein Interesse für Unternehmenskulturen geweckt hat, sowie Franz Rohrer vom BKA-KI 12, der meine Fragen zur Wirtschaftskriminalität kompetent und ausführlich beantwortete, zu Dank verpflichtet.

Für Literaturhinweise und Korrekturvorschläge bedanke ich mich bei Jürgen Dollinger vom Chaos Computer Club ERFA-Kreis Ulm, Uwe Jendricke (Telematik Universität Freiburg), Andreas Borchert (SAI Universität Ulm), Julia Herfordt im Bereich Wirtschaftspsychologie (Psychologie Universität Köln), Claudia Wortmann (Kulturwissenschaften Universität Hildesheim) sowie Christian Ehrhardt (SAI Universität Ulm) für seine Hilfe bei LaTeX.

Sven Übelacker

Inhaltsverzeichnis

1 Einführung

Wirtschaftskriminalität nimmt seit Ende des Kalten Krieges weltweit einen immer größeren Stellenwert ein. Dabei sind viele Unternehmen nur dürftig geschützt. Durch die weitgehende digitale Vernetzung kommen neue Gefahren auf Unternehmen zu, die eine neue Dimension der Kriminalität darstellen. Mit Sicherheitsanwendungen auf IT-Ebene wird versucht Cybercrime zu begegnen.

Doch sollte der Blick nicht immer auf externe Gefahren gerichtet sein: Innentäter sind nicht zu unterschätzen und brauchen keine gut administrierten Firewalls zu umgehen. Hier spielt das Verhältnis zwischen Mitarbeiter und Unternehmen eine wichtige Rolle, also inwiefern sich ein Mitarbeiter mit seinem Unternehmen identifizieren kann. Großen Einfluss hierauf hat die vorherrschende Unternehmenskultur, in der sich sowohl – teilweise rituell geprägte – Umgangs- und Kommunikationsformen als auch Führungsstile manifestieren.

Die Arbeit soll einerseits einen Überblick über die IT-Gefahren und ihren Lösungsmöglichkeiten geben, die die Unternehmensicherheit erhöhen, andererseits aber auch funktionale und dysfunktionale Effekte von Unternehmenskulturen hinterfragen.

Die Gefahren der Wirtschafts- und Computerkriminalität werden in diesem Kapitel anhand von Statistiken und Studien (1.2) dargelegt. Die steigende Bedrohung aus dem Internet kann am repräsentativsten mit der Grafik der sicherheitsbedrohenden Vorfälle, die dem CERT[i] / Coordination Center ↪**1** von 1988 bis 2001 gemeldet wurden, in Abb. 1.1 deutlich gemacht werden.

Die neu entstanden Formen der Kriminalität (1.4) müssen analysiert und ihre juristischen Konsequenzen (1.6) sowie die Motive für Computerangriffe (1.5) beschrieben werden.

Zuerst jedoch gilt es, den Begriff der „Sicherheit“ zu klären:

---

i steht für „Computer Emergency Response Team“; mehr über das CERT unter 2.2.1

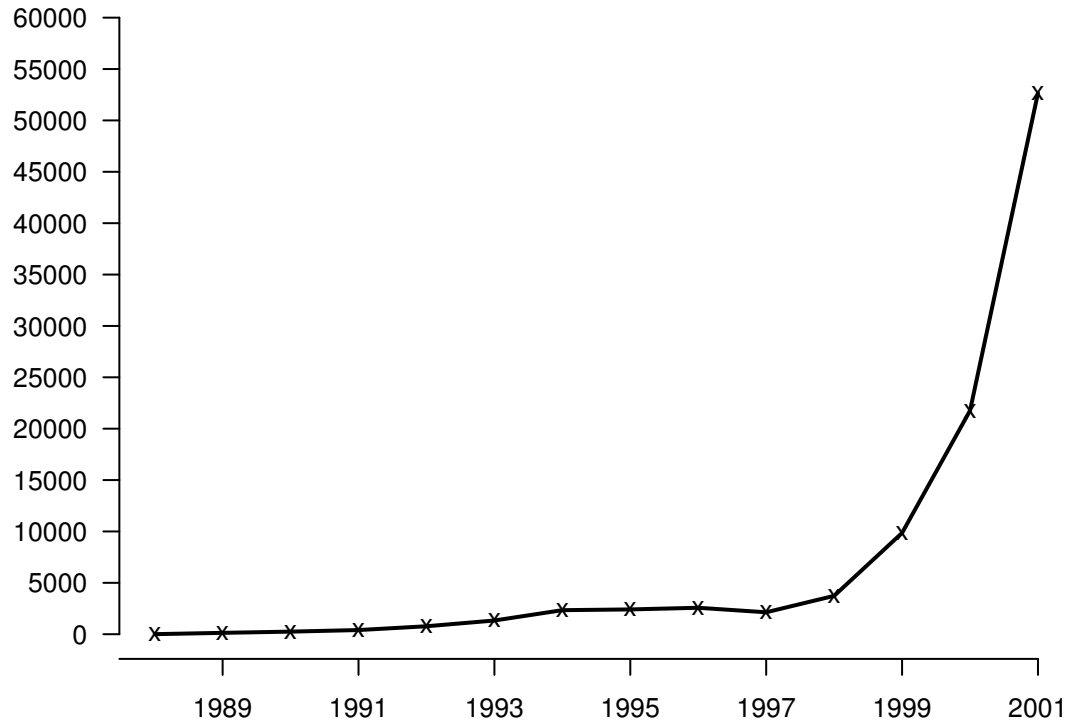

Abbildung 1.1: Number of incidents reported to CERT
(Quelle: CERT/Coordination Center Statistics 1988–2001)

1.1 Der Sicherheitsbegriff ...

Für das deutsche Wort „Sicherheit“ gibt es bei der Übersetzung ins Englische gleich mehrere Begriffe, wie etwa „Security“, „Safety“ oder auch „Certainty“. Alle geben einen Teil des deutschen Sicherheitsbegriffs wider, so sind für den Computerbereich die beiden Wörter „Security“ und „Safety“ von Belang.

Ersterer wird meist im IT-Bereich benutzt und drückt den Schutz vor Crackerangriffen[ii] oder Viren – also die Maßnahmen gegen ungewollter Nutzung, Sabotage oder Einbruch in ein Computersystem – aus. Auf diesen Sicherheitsbegriff werde ich hier eingehen und zur besseren Differenzierung von den anderen als IT-Sicherheit bezeichnen.

„Safety“ wird im Kontext des Schutzes vor physischem Schaden benutzt, um beispielsweise Anforderungen an Abstrahlung eines Bildschirmes zu stellen, die den Benutzer schaden könnte, oder Richtlinien, um die Brandgefahr zu senken.

IT-Sicherheit bzw. Unternehmensschutz ist ganzheitlich zu sehen und hat neben der technischen auch eine sozialwissenschaftliche Komponente. Aus diesem Grunde werden beide Seiten behandelt.

1.1.1 ... in der Informatik

In der technischen Informatik[iii] [Egg96] werden unter Sicherheit drei Dimensionen verstanden, weshalb auch vom „Sicherheitswürfel“ (siehe auch [Str91, S. 81]) gesprochen wird, dessen Dimensionen je nach Sparte verschiedene Gewichtung erfahren:

- **Vertraulichkeit:** Daten, insbesondere personenbezogene Daten, müssen im Verkehr vertraulich behandelt werden. Dazu wird jede Stufe der Vertraulichkeit in einer Klasse definiert: „unclassified“ (offen), „restricted“ (Verschluss), „confidential“ (vertraulich), „secret“ (geheim) sowie „top secret“ (streng geheim).
- **Integrität:** Der Grad der Integrität von Daten beschreibt die Anforderung, wie korrekt, vollständig sowie aktuell sie dem Original (z.B. beim Datentransfer) entsprechen, also wie stark sie vor unauthorisierter Manipulation geschützt sind. Man unterscheidet zwischen hoher, mittlerer und niedriger Integrität.
- **Verfügbarkeit:** Der Benutzer sollte möglichst (zeitlich) uneingeschränkt auf

ii Die Begriffe „Hacker“ und „Cracker“ werden in 1.3 erklärt.
iii Auf die technischen Sicherheitsaspekte wird in Kap. 2 näher eingegangen.

die für ihn authorisierten Computerressourcen zugreifen können. Wie wichtig welche Ressourcen sind, wird durch eine Klassifikation in „essentiell“, „erwünscht“ und „unwichtig“ vorgenommen.

Wichtig ist in diesem Zusammenhang die Erkenntnis, dass Sicherheit einen Prozess darstellt, der kontinuierlich verfolgt werden muss; d.h. ein heute sehr hohes Sicherheitsniveau kann morgen schon unsicher sein. Ebenfalls sind Sicherheitskomponenten mit Kettengliedern zu vergleichen, denn ein Sicherheitssystem kann nur so sicher sein, wie seine schwächste Komponente. [Sch00]

1.1.2 ... in den Sozialwissenschaften

Zu den technischen Sicherheitsaspekten kommen als Unterstützung und Ergänzung die sozialen Praktiken des verantwortlichen Umgangs mit Daten hinzu. Sensible Daten können nicht ausschliesslich durch gute technische Sicherheitsmaßnahmen geschützt werden, es bedarf ebenfalls einer Sensibilisierung der Benutzer und des Managements, der Organisation und Verteilung der Verantwortung. Dazu gehören sowohl die Anzahl risikobehafteter Anwendungen und der Schweregrad sowie die Korrigierbarkeit von Vorfällen als auch die Kontrollierbarkeit des Risikos. Als etwas neuere Aspekte kann hier noch das Krisenmanagement und die Risikokommunikation [GO94, GO95, Obe99a] genannt werden.

Als einen wichtigen Punkt des Unternehmensschutzes beschäftigt sich Kap. 3 mit der Identifikation des Mitarbeiters mit seinem Unternehmen bzw. mit dem Einfluss von Unternehmenskulturen auf die Unternehmenssicherheit.

1.2 Status Quo

Um über die Ländergrenzen hinaus zu gehen und um zwischen Computer- und Wirtschaftskriminalität sowie Cybercrime vergleichen zu können, werden folgende Untersuchungen zu Rate gezogen:

Die Polizeiliche Kriminalstatistik 2001 (PKS) für Deutschland, die über die *erfassten* Fälle und deren Aufklärungsquote von Computerkriminalität berichtet und nur das Hellfeld beschreiben kann. Hier können auf jeden Fall Rückschlüsse auf den Erfolg der Strafverfolgung sowie die Tendenzen der Computerkriminalität gezogen werden, da die Zahlen von 1987 bis 2001 vorliegen. Zu diesem Zweck wurde hier die grafische Darstellung gewählt.

Gefolgt wird die PKS von der „Europäische Umfrage Wirtschaftskriminalität 2001“ von PricewaterhouseCoopers, eine sehr ausführliche Arbeit, die auch die Wahrnehmung und die tatsächliche Häufigkeit von wirtschaftskriminellen

Handlungen untersucht. Zuletzt wird der US-amerikanische „Computer Crime and Security Survey 2002“ von CSI und FBI vorgestellt.

Nur kurz ausführt wird an dieser Stelle die KES/KPMG Sicherheitsstudie 2002 ↪**2**, in der 91% der Befragten aus großen deutschen Unternehmen den Image-Verlust durch Computerkriminalität als Faktor „wichtig“ oder „sehr wichtig“ einstuften. Die Rangfolge der IT-Gefahren blieb wie in den vorigen Studien gleich:

1. menschliches Versagen
2. Datenunfälle durch Technikfehler
3. Malware, d.h. Viren[iv], Würmer und Trojanische Pferde
4. Angriffe durch Hacker, Wirtschaftsspione oder Saboteure

1.2.1 Polizeiliche Kriminalstatistik 2001 (D)

Die im Mai 2002 von der Bundesinnenministerkonferenz unterzeichnete und vom Bundeskriminalamt (BKA) erstellte Polizeiliche Kriminalstatistik (PKS) [Bun01b] weist neben allen anderen Statistiken auch die Computerkriminalität unter Schlüssel 8970 aus. Er ist untergliedert in weitere Schlüssel, die zusammen die Computerkriminalität ergeben (siehe Tab. 1.1).

Die Computerkriminalität hat von 2000 auf 2001 um 39,9% zugenommen, im gleichen Jahreszeitraum davor waren es 25,0%, d.h., dass jetzt die Häufigkeitszahl[v] bei 96,4 liegt. Im Vorjahr waren es 69,0. Es liegt also eine klare Steigerung der Computerkriminalität vor, dessen Unterschlüssel im folgenden untersucht werden.

Den größten Anteil macht jedes Jahr der Kartenbetrug (Schlüssel 5163) aus, weshalb er in Abb. 1.2 extra ausgewiesen wurde. Er hat aber das kleinste Wachstum verglichen mit den anderen Unterschlüsseln. Weitere Grafiken sind zur Aufklärungsquote (Abb. 1.3), zur Computersabotage (Abb. 1.4, Seite 21) sowie über das Ausspähen von Daten (Abb. 1.5, Seite 22) erstellt worden.

Starkes Wachstum verzeichnen die unter „Ausspähen von Daten“ sowie „Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung“ laufenden Straftaten: Die letzten zwei Jahre mehr als eine Verdoppelung der

iv Der durchschnittliche Schaden pro Virenangriff wird mit ungefähr €26.000 pro Unternehmen beziffert [SH02].

v Fälle pro 100.000 Einwohner

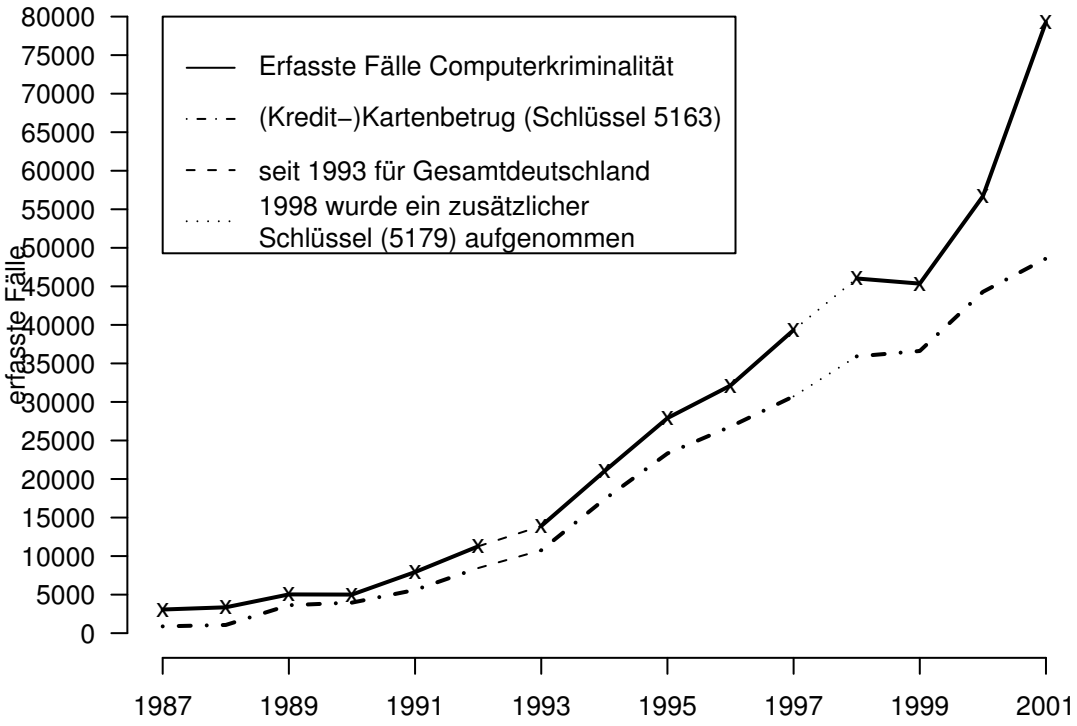

Abbildung 1.2: Erfasste Fälle der Computerkriminalität in Deutschland
(Quelle: Polizeiliche Kriminalstatistik des BKA der jeweiligen Jahre [Bun01b])

Schlüssel	Beschreibung	1999/2000	2000/2001
5163	Betrug mittels rechtswidrig erlangter Karten für Geldausgabe- bzw. Kassenautomaten	21,0%	9,8%
5175	Computerbetrug – § 263a StGB	47,5%	**162,3%**
5179	Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	55,7%	**265,7%**
5430	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung – §§ 269, 270 StGB	**116,1%**	**243,4%**
6742	Datenveränderung, Computersabotage – §§ 303a, 303b StGB	69,9%	68,0%
6780	Ausspähen von Daten	**156,2%**	**171,9%**
7151	Softwarepiraterie (private Anwendung z.B. Computerspiele)	40,0%	} -9,4%
7152	Softwarepiraterie in Form von gewerbsmäßigen Handelns	-25,2%	

Tabelle 1.1: Zusammensetzung des Schlüssels 8970 (Computerkriminalität)
(Quelle: Polizeiliche Kriminalstatistik des BKA der jeweiligen Jahre [Bun01b])

Taten. Doch auch „Computerbetrug“ und „Betrug mit Zugangsberechtigungen“ haben im letzten Jahr zugenommen.

Die Aufklärungsquote (siehe Abb. 1.3) liegt bisher immer um die 50%, doch interessant ist, dass sie bei der Softwarepiraterie (Schlüssel 7151 und 7152) über 95% beträgt, wodurch vielleicht auch der Rückgang dieser Straftat mit zu erklären ist.

In der PKS aus dem Jahr 2000 liegt ebenfalls eine Tabelle über die Alterstruktur vor: So waren von den 14.848 untersuchten StraftäterInnen über 65% älter als 21 Jahre. Insgesamt wurden davon 78,3% Männer und 21,7% Frauen straffällig.

1.2.2 PwC-Umfrage Wirtschaftskriminalität 2001 (EU)

3.403 Unternehmen, gemeinnützige Organisationen und staatliche Einrichtungen aus 15 Ländern in Europa wurden in der „Europäischen Umfrage zur Wirtschaftskriminalität 2001“ [MS01] von PricewaterhouseCoopers ↪**3** befragt. Unter ihnen sind 1.492 international und 1.560 national tätige Unternehmen sowie 351 staatli-

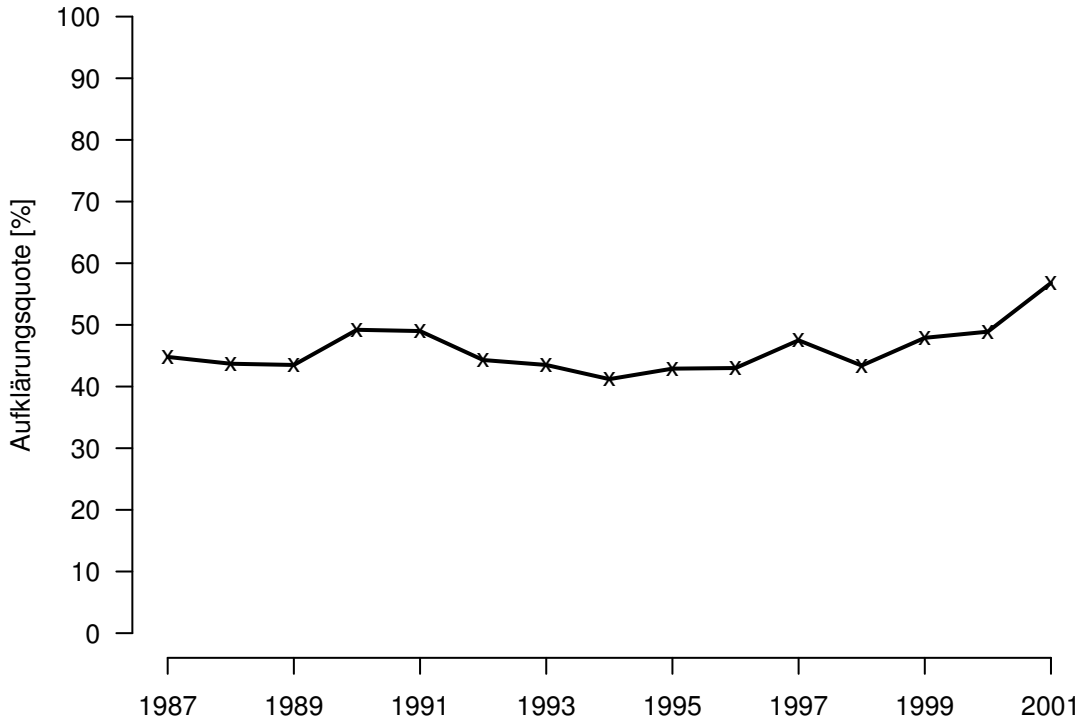

Abbildung 1.3: Aufklärungsquote der Computerkriminalität in Deutschland
(Quelle: Polizeiliche Kriminalstatistik des BKA der jeweiligen Jahre [Bun01b])

che Einrichtungen und Non-Profit-Unternehmen zu finden.

Die am stärksten verbreiteten Deliktformen sind in Deutschland (Europa) Unterschlagung 74,5% (63%), Vertrauensbruch 21,3% (24,0%), Cybercrime 10,6% (13,0%), Korruption 8,5% (11,0%), Erpressung 4,3% (5,0%) und Geldwäsche 2,1% (5,0%); d.h., dass die beiden führenden dolosen Handlungen intern ausgelöst werden: Vertrauensbruch wird vom Management und Unterschlagung von Mitarbeitern begangen.

Schadenshöhe

Unter den befragten Unternehmen gab es 854, die in den letzten beiden Jahren von Wirtschaftskriminalität betroffen waren, von denen wiederum 513 eine Aussage über die Kosten doloser Handlungen machten. Unternehmen mit weniger als 5.000 Beschäftigten hatten zusammengenommen einen Gesamtverlust von € 1.038.900.000 und Unternehmen mit mehr als 5.000 Beschäftigten € 2.597.315.000 zu beklagen; das macht zusammen € 3,6 Milliarden in zwei Jahren. Durchschnittlich musste also jedes betroffene Unternehmen mit einer Schadenshöhe von ca. € 6,7 Mio.[vi] rechnen.

Folgeschäden

Neben dem monetären Schaden erfährt ein Unternehmen bei Bekanntwerden doloser Handlungen meist Folgeschäden, wie Imageverlust, die aber schwer zu quantifizieren sind. „Ein Versagen bei der Bekämpfung wirtschaftskrimineller Handlungen kann die Keimzelle für langfristig wirkende Probleme darstellen."

In der Studie wird versucht, mithilfe der Einteilung in „Stabilität der Geschäftsbeziehungen", „Mitarbeitermoral", „Reputation" und „Börsenkurs" eine Aussage zu treffen (Tab. 1.2). Heraus sticht der große, negative Einfluss auf Mitarbeitermoral und Geschäftsbeziehungen, den die Befragten als sehr kritisch einstuften. Dagegen scheint es vergleichsweise wenig und in Deutschland keine Auswirkungen auf den Börsenkurs zu geben.

Regionale Unterschiede

In der Studie werden in west- und osteuropäisch beheimatete Unternehmen unterschieden. Es stellt sich heraus, dass sich der Anteil der Unternehmen, die Opfer von Wirtschaftskriminalität wurden, in dieser Einteilung deckt: In osteuropäische

vi Das heisst, bei Unternehmen mit weniger als 5.000 Beschäftigten € 3,1 Mio. und bei Unternehmen mit mehr als 5.000 Beschäftigten € 15,1 Mio. in zwei Jahren (≙ € 20.000 pro Tag).

Negative Auswirkungen auf	Unternehmen in Europa	Unternehmen in Deutschland
Stabilität der Geschäftsbeziehungen	**29,5%**	**43,5%**
Mitarbeitermoral	**35,9%**	**40,0%**
Börsenkurs	3,5%	0,0%
Reputation	16,3%	10,1%
Sonstiges	14,8%	15,6%

Tabelle 1.2: Folgeschäden durch Wirtschaftskriminalität
(Quelle: Europäische Umfrage zur Wirtschaftskriminalität 2001 [MS01])

Ländern wurden 26% (623 Unternehmen) und in westeuropäischen Ländern 29% (2433 Unternehmen) der Unternehmen von dolosen Handlungen heimgesucht. In Osteuropa kommen 49% der Delikte aus dem Betrieb – d.h. 51% werden extern begangen –, was darauf hindeutet, das spiegelt eine stärkere Verbreitung von Korruption[vii] als in westeuropäischen Staaten wider (Westeuropa: 39% extern, 61% intern).

Wahrnehmung

Die Einschätzung der Befragten zur Anzahl der Straftaten unterscheidet sich in allen Fällen von den tatsächlichen Zahlen. Diese Gegenübergestellung zeigt die Diskrepanz zwischen der Wahrnehmung und der Realität.

Aus Tab. 1.3 ist ersichtlich, dass Unterschlagung, Vertrauensbruch und Cybercrime deutlich unterschätzt, wo hingegen Korruption sowie Geldwäsche überschätzt werden. Die Wahrnehmung spielt aber eine wichtige Rolle bei der Prävention von Straftaten.

Anfälligkeit & Unternehmenskultur

Aus der Studie geht hervor, dass größere Unternehmen anfälliger für wirtschaftskriminelle Handlungen sind. Als allgemeines Problem wird die Identifikation des Mitarbeiters mit seinem Unternehmen gesehen, was aber bei großen Firmen sich stärker auswirkt, da keine „personifizierbaren Opfer“ existieren. So wurden 35,9% der deutschen Unternehmen mit weniger als 5.000 Mitarbeitern und 73,2% der Unternehmen mit mehr als 5.000 Mitarbeitern Opfer wirtschaftskrimineller

vii „Korruption ist eine Form der Wirtschaftskriminalität, die per definitionem Externe involviert.“ [MS01]

Dolose Handlung	Einschätzung	Tatsächliche Verbreitung
Unterschlagung	**29%**	**63%**
Vertrauensbruch	**9%**	**24%**
Cybercrime	**6%**	**13%**
Korruption	23%	11%
Geldwäsche	12%	5%
Erpressung	2%	5%

Tabelle 1.3: Wahrnehmung und tatsächliche Verbreitung in Europa
(Quelle: Europäischen Umfrage zur Wirtschaftskriminalität 2001 [MS01, S. 12])

Handlungen. Am Anfang der Studie wird eine starke Unternehmenskultur zur Prävention und Abschreckung propagiert, doch „stark“ wird hier leider nicht weiter erläutert noch wie eine derartige Unternehmenskultur geprägt sein sollte.

Neben der Identifikation gehen große Unternehmen höhere Risiken ein, um auf (neuen) Märkten ihre Wachstumschancen auszubauen. Die Delegation der operativen Geschäftsführung und die komplexere Ablauforganisation tragen ihr übriges dazu bei (Kontrollverlust).

1.2.3 Computer Crime and Security Survey 2002 (USA)

Das 1974 gegründete Computer Security Institute (CSI ↪**4**) und das FBI ↪**5** in ihrer regionalen Abteilung des Computer Intrusion Squad in San Francisco geben jährlich die Ergebnisse der Umfrage „Computer Crime and Security Survey“ [Pow02] unter Sicherheitstechnikern heraus, die in US-amerikanischen Konzernen, Universitäten, Regierungseinrichtungen und medizinischen Instituten beschäftigt sind. 2002 antworteten 503 Experten (1998: 520; 1999: 522; 2000: 643; 2001: 534) über die Anzahl und Arten sowie Schäden der Angriffe.

- 90% der Befragten hatten in den letzten 12 Monaten Sicherheitsverletzungen
- 80% hatten finanziellen Schaden durch Einbrüche
- 44% gaben Antwort über den finanziellen Schaden, der sich insgesamt auf $ 455.848.000 beläuft
- 34% erstatteten Anzeige (1996: 16%)
- 2002 bezeichnen die Befragten zu 74% das Internet und 33% das interne System als „point of attack“. Das ist eine Steigerung des Internetanteils seit fünf Jahren in Folge.

52% nutzen ihre Internet-Präsenz zum E-Commerce, von denen 38% einen Missbrauch bzw. nichterlaubten Zugriff feststellten und 21% nicht wussten, ob sie Opfer eines Angriffs waren. Die Rangliste der Arten der bekanntgewordenen Attacken liest sich wie folgt:

- 70% Vandalismus (2000: 64%)
- 55% Denial of Service (2000: 60%)
- 12% Diebstahl von Transaktionsinformationen
- 6% Finanzbetrug (2000: 3%)

Das Federal Bureau of Investigation (FBI) hat eigens für die infrastrukturelle Sicherheit das NIPC ↪**6** als „Joint Partnership“ zwischen US-amerikanischer Industrie und Bundesbehörden ins Leben gerufen.

1.2.4 Vergleich der Studien

Terminologie

Die in den Publikationen genannten Termini Cybercrime, Wirtschaftskriminalität und Computerkriminalität beschreiben verschiedene Kategorien doloser Handlungen. Am weitesten ist der Begriff *Wirtschaftskriminalität* gefasst; er beschreibt die gesamten kriminellen Taten, die die Wirtschaft bedrohen, und beinhaltet auch Teile der Computerkriminalität und des Cybercrime.

Computerkriminalität – im Englischen „Computer Related Crime“ genannt – besteht aus den in der PKS [Bun01b] aufgeführten dolosen Handlungen; in der Veröffentlichung [SCJ00] von Vogon International ↪**7** wird außerdem „White Collar Crime“ erwähnt, d.h. die Computerkriminalität umreisst folgende Punkte:

- (Kredit-)Kartenbetrug
- Ausspähen von Daten
- Softwarepiraterie
- White Collar Crime
- Computer Misuse/Abuse/Fraud
- IT Fraud
- Internet Abuse/Misuse

Ein Teil der Computerkriminalität wird vom *Cybercrime* ausgemacht, der sowohl als Penetration durch Denial-of-Service (DoS) Angriffe und Cracker-Einbrüche als auch Verbreitung von Viren und Würmern über das Internet verstanden wird.

Dunkelfeld und Perzeption

Die PKS stellt als einzige der vorgestellten Studien eine Statistik der erfassten Straftaten in der Computerkriminalität in Deutschland dar, von denen um die Hälfte aufgeklärt werden können. Die CSI/FBI Studie benennt bei ihrer Umfrage, dass ca. ein Drittel der von Unternehmen in den USA wahrgenommenen Straftaten der Cybercrime überhaupt angezeigt werden[viii]. Natürlich können nicht so ohne weiteres von den USA auf Deutschland Rückschlüsse getroffen werden, was aber hier zu zeigen wäre, ist, dass eine Schätzung über die Dunkelziffer der Straftaten abgegeben bzw. dass mit ausreichend vielen Umfragen das Dunkelfeld erschlossen werden könnte.

Wie unterschiedlich die Wahrnehmung und die tatsächliche Verbreitung von wirtschaftskriminellen Vorfällen ist, lässt die EU-Studie von Pricewaterhouse-Coopers [MS01] dadurch erkennen, dass die ersten drei ausschlaggebendsten dolosen Handlungen – nämlich Vertrauensbruch, Unterschlagung und Cybercrime – unterschätzt werden. Durch eine verminderte Risikowahrnehmung ist es noch schwieriger, ein Unternehmen zu schützen. Zumal durch ein einmal stattgefundener Vorfall die Mitarbeitermoral derart sinken kann, dass zwar eine Wahrnehmung des Risikos vorhanden, doch bedingt durch eine schwächere Identifikation mit dem Unternehmen die Bereitschaft einzugreifen und den Vorfall zu melden geringer wird.

Trotz der weitverbreiteten Angst vor einem Image-Schaden (siehe KES/KMPG Sicherheitsstudie, „The Enemy Within“ [SCJ00]) wird wenig unternommen dem vorzubeugen.

Bedrohung durch Cybercrime

Cybercrime macht in der EU-Befragung von PricewaterhouseCoopers zur Wirtschaftskriminalität 10,6% aus und steht an dritter Stelle in der Rangliste der häufigsten Vorfälle, was aber externe Taten angeht, führt Cybercrime an erster Stelle noch vor Korruption (8,5%) die Rangliste an. In Deutschland gab es laut PKS vom Jahr 2000 auf das Jahr 2001 eine Steigerung der Computerkriminalität von fast 40%.

viii Zum Vergleich: Das aus dem Bereich der Beweismittelsicherung (Computer Related Crime) stammende Unternehmen Vogon International hat in seinem Bericht „The Enemy Within“ [SCJ00] festgestellt, dass 8 von 10 Geschädigten die Tat aus Furcht vor negativer Publicity nicht anzeigen.

Das macht deutlich, dass die Computerkriminalität und damit auch der anteilige Cybercrime jetzt und auch weiterhin eine bedeutende Rolle spielen wird.

Bei der Umfrage von CSI und FBI sind genauere Informationen zu finden: Da es sich hier um Cybercrime handelt, der vorwiegend extern begangen wird, liegt der Internetanteil bei 74% der Taten deutlich vor internen Tätern. 90% der befragten Unternehmen hatten Sicherheitsverletzungen in den letzten zwölf Monaten, davon 80% auch einen finanziellen Schaden. Von den Attacken waren 70% vandalistischer Natur, 55% Denial-of-Service (DoS) Attacken, die auch unter die destruktiven Taten eingeordnet können. Unternehmen, die sich also auf E-Commerce spezialisiert haben, sind besonders gefährdet, wenn von den 90% Sicherheitsverletzungen ausgegangen werden darf.

Über IT-Gefahren, Lösungsansätze und Sicherheitsstandards wird in Kap. 2 berichtet.

Bedrohung durch Innentäter

Interne Formen der Wirtschaftskriminalität, wie Unterschlagung (74,5%) oder Vertrauensbruch (21,3%), führen die Rangliste von PricewaterhouseCoopers an, und machen den internen Faktor mehr als deutlich. Auch die KES/KPMG Sicherheitsstudie zeigt, dass menschliches Versagen an erster Stelle steht.

Aus diesem Grund wird bei PricewaterhouseCoopers auch eine „starken Unternehmenskultur“ erwähnt, die diese Risiken besser beherrschen soll. Damit ist gemeint, dass eine Unternehmenskultur und die daraus resultierende Art der Identifikation des Mitarbeiters mit seinem Unternehmen das Niveau der Risikowahrnehmung und -kommunikation beeinflusst. Was genau eine (starke) Unternehmenskultur ausmacht, also ihre funktionalen und dysfunktionalen Effekte, wird in Kap. 3 behandelt.

1.3 Von Hackern und Crackern

Für die Unterscheidung zwischen „guten“ und „bösen“ Hackern hat sich folgende Definition ↪**8**, die hier verwendet werden soll, herausgebildet: Hacker, auch „White hats“ genannt, sind enthusiastische, technikbegeisterte Menschen. Sie versuchen, Sicherheit zu schaffen, indem sie nach Sicherheitslücken suchen, die sie aber nicht missbrauchen; sie versuchen sie zu schließen und informieren die Öffentlichkeit darüber. Sie gelten als die „Guten“, die sich selbst eine Hackerethik gegeben haben. Bei IBM gibt es sogar die Berufsbezeichnung „Ethical Hacker“ [RC01], weshalb auch vom „Ethical Hacking“ [SO02] gesprochen wird.

Cracker hingegen stellen die „Bösen“ dar; sie werden auch als „Black hats“ bezeichnet und suchen ebenfalls nach Sicherheitslücken, nutzen diese aber für ihre eigenen (illegale) Zwecke.

1.4 Neue Charakteristika der Kriminalität

Alle kriminellen Ziele der realen Welt, wie Betrug, Diebstahl oder Sabotage, existieren auch im Internet. Bei Diebstahl stelle man sich am besten das Entwenden von geistigem Eigentum vor, da es kein materielles Gut ist und deshalb unbegrenzt kopiert werden kann. Der wesentliche Unterschied jedoch besteht nach Bruce Schneier [Sch00, 17ff.] in **drei** zusätzlichen Charakteristika, die nur durch die Computerisierung und das Internet möglich wurden:

Die Wahrscheinlichkeit des Gelingens eines Angriffs verliert durch die **„Automation“ (1.)** der Vorgänge an Bedeutung, das gleiche gilt auch für den zeitlichen Aufwand: Eine Geldbörse zu stehlen wird nur „rentabel“ für den Dieb, wenn sich das Verhältnis von benötigter Zeit und Erfolg „rechnen“. Anders sieht es in der vernetzten Welt aus: Ein Angriff kann schnell („Permanenz der Handlung“ bzw. „zeitliche Autonomie“ [Jae98]) und automatisiert durch Scripte durchgeführt werden. Der Dieb braucht nur zu warten, bis das Geld bei ihm ankommt. Auch bei geringeren Beträgen lohnt sich dieser Aufwand.

Ausserdem ist eine physische Anwesenheit am Tatort nicht mehr zwingend notwendig. So eine Attacke wird auch als **„Action at a Distance“ (2.)** [Sch00] oder „ubiquitäre Tat“ [Jae98] bezeichnet. Das Internet hat keine Grenzen. Die Probleme der Strafverfolgung liegen hierin begraben. Man könnte meinen, dass Straftaten vornehmlich aus Staaten begangen werden, in denen schwache Gesetze gegen Computerkriminalität existieren. Nach einer Studie von Riptech Inc. ↪**9** kommen die meisten Cyber-Attacken aus den USA (Tab. 1.4) und bezogen auf die Anzahl der Internetnutzer aus Israel (Tab. 1.5) [BY02]. Doch an zweiter Stelle kommen asiatische Länder, weshalb in der Untersuchung [Smi02] von Predictive Systems Inc. ↪**10** die These vertreten wird, dass Cracker unsichere asiatische Server nutzen, um von dort aus weitere Angriffe durchzuführen (siehe auch [Lem02]).

Unter **„Technique Propagation“ (3.)** versteht Bruce Schneier, dass nur der erste Angreifer die Erfahrung besitzen muss, um einen erfolgreichen Angriff durchführen zu können. Alle nachfolgenden können auf dieses technische Wissen respektive auf fertige Scripte im globalen Dorf zurückgreifen. Dadurch ist auch das abfällige Wort „Script Kiddies“ – insbesondere bei distributed Denial-Of-Service Angriffen – für Jugendliche entstanden, die nur Programme ausführen, ohne vom

Rang	Land	Attacken
1.	USA	29,6%
2.	Südkorea	8,8%
3.	China	7,8%
4.	Deutschland	5,9%
5.	Frankreich	4,5%
6.	Kanada	3,9%
7.	Taiwan	2,6%
8.	Italien	2,5%
9.	Großbritanien	2,5%
10.	Japan	2,0%

Tabelle 1.4: Top Ten der Ursprungsländer der Attacken insgesamt

Rang	Land	Attacken
1.	Israel	26,16%
2.	Hong Kong	14,50%
3.	Thailand	11,57%
4.	Südkorea	10,03%
5.	Frankreich	8,60%
6.	Türkei	7,85%
7.	Malaysia	7,74%
8.	Polen	7,52%
9.	Taiwan	7,10%
10.	Dänemark	7,07%

Tabelle 1.5: Top Ten der Urspungsländer der Attacken pro 10.000 Internetbenutzer

(Quelle: Riptech Internet Security Threat Report [BY02])

technischen Hintergrund Ahnung zu haben.[ix] Doch ist für sie dies meist ein Einstieg, das System besser kennenzulernen.

Stefan Jaeger [Jae98] sieht neben den o.a. neuen Charakteristika durch Vernetzung noch fehlende Sicherheitsstandards sowie die geringe Wahrscheinlichkeit der Entdeckung einer Tat als Risikofaktoren für eine der Ursachen steigender Computerkriminalität. Auch ist die Höhe des Schadens nicht mehr an die physischen Verfügbarkeit der Tatbeute gebunden (Beispiel: Geldtransporter oder Banktresor). Sie kann also höher liegen als bei klassischen Straftaten.

Die bislang gebräuchlichen Sicherheitsstandards ITSEC und Common Criteria werden in Kapitel 2.3 (Seite 37) ausführlich beschrieben. Die in den Polizeilichen Kriminalstatistiken des BKA erfassten Straftaten im Computerbereich entsprechen nur dem Hellfeld, die Dunkelziffer muss wesentlich höher liegen [Jae98], da ein Bekanntwerden meist mit einem Image-Verlust (siehe Kap. 1.2.4) für das Unternehmen verbunden ist. Außerdem lag die Aufklärungsrate in Deutschland bisher immer unter 50% (siehe hierzu Abb. 1.3 und Kap. 1.2.1).

Alle diese neuen Möglichkeiten zusammengenommen zeigen das Gefahrenpo-

ix In der Newsgroup `de.org.ccc` fand sich vor ein paar Jahren die Bitte eines Users, einen Rechner mit der IP `127.0.0.1` (localhost) anzugreifen, was auch einige taten. Das Geschrei war groß, als sie merkten, dass es ihre eigenen Rechner waren.

tential der virtuellen Kriminalität.

1.5 Motive der Computerangriffe

Was veranlasst Menschen Computerangriffe durchzuführen? Bruce Schneier beschreibt in seinem Buch „Secrets & Lies“ [Sch00] eine Klassifikation in kriminelle Angriffe sowie in Aktionen um den Bekanntheitsgrad zu steigern.

1.5.1 Kriminelle Attacken

Kriminelle Handlungen existieren natürlich auch im Internet; um einige zu nennen: (Finanz-)Betrug, destruktive Attacken, Diebstahl geistigen Eigentums und Diebstahl der Identität. Alle haben das Ziel sich einen Vorteil zu verschaffen, sei es finanzieller Art oder, um die „andere“ Seite zu schwächen. Die andere Seite kann hier die Konkurrenz sein, aber auch Angriffe ideologischer, religiöser, politischer oder martialischer Art sind nicht nur denkbar, sondern werden sogar angewandt.

Zerstörerische Taten haben eine lange Tradition in der realen Welt, beispielsweise die mehrfachen Brandstiftungen der Bibliothek von Alexandria, die Julius Caesar im Jahre 47 vor Christi als erster verwüsten ließ. Ein aktuelleres Beispiel ist der US-amerikanische Angriff auf die Kommunikationssysteme Iraks während des Golfkrieges. In der vernetzten Welt entwickelt sich seit einiger Zeit im militärischen Bereich verstärkt der sog. „Information Warfare“, d.h. Kriegsführung mithilfe der Informationstechnologie. Bei den zerstörerischen Taten spielen Profitinteressen eine geringere Rolle.

Häufig ist zur Zeit in der öffentlichen Diskussion der **Diebstahl geistigen Eigentums**, gemeint ist damit neben dem sehr weit verbreiteten illegalen Kopieren von Multimediadaten und Software[x] auch der Diebstahl von Betriebsgeheimnissen, wie Prototypen und Forschungsergebnisse sowie zukünftige Patent- und Gebrauchsmuster. Der große Unterschied zur realen Welt besteht jedoch in der unbegrenzten Fähigkeit digitale Dokumente zu kopieren respektive zu „stehlen“, ohne sie physikalisch zu entwenden. Die Qualität bleibt gleich, es entsteht sozusagen eines neues Original.

x In Kanada besteht die Hälfte aller verwendeten Software aus Raubkopien, in China sind es 95%, in Vietnam 98% [Sch00, S. 25]

Identitätsdiebstahl[xi] wird verwendet, um sich als jemand anderes auszugeben. Das kann verschiedene Gründe haben: Einmal die wahre Person mit etlichen Bestellungen zu überhäufen und zu schädigen, oder auf Kosten anderer einzukaufen, wie z.B. der Benutzung fremder Kreditkarteninformationen (Inhaber, Kreditkartennummer und Ablaufdatum), die entweder mittels Programmen generiert oder aus dem Datenstrom gesnifft wurden. Es ist also wesentlich einfacher die Kreditkarteninfos aus dem Internet zu bekommen und diese dort anzuwenden, als die Karte (physikalisch) entwenden zu müssen. Dieser Tatbestand des Betruges nimmt stetig zu.

Es reicht z.B. schon aus, die E-Mail-Adresse eines Opfers zu kennen, um diesen Account mit Massen-E-Mails unbrauchbar zu machen, indem man sich mit der fremden Adresse in vielen Mailinglisten einträgt, die ein hohes Aufkommen an Beiträgen aufweisen und bei denen man sich ohne Rückfrage anmelden kann. Ganz intelligente Mailbombing-Angreifer setzen Kettenbriefe in Gang, bei denen je ein Exemplar an die E-Mail-Adresse des Opfers gemailt werden soll; also Hilferufe von krebskranken Kindern oder E-Mails über kostenlose Handys etc., die von Newbies im Netz gern weiterverbreitet werden.

1.5.2 Nur aus Publicity-Gründen...

Bei dieser Art Attacke geht es dem Angreifer ausschließlich um die Steigerung seines Bekanntheitsgrads. Dieses altbekannte Phänomen – man denke hierbei an die Ermordung von Persönlichkeiten, wie der von John Lennon, oder die Zerstörung kultureller und historischer Güter, wie der Artemis-Tempel[xii] im Alten Griechenland – hat sich logischerweise auch auf die Neuen Medien übertragen. Dabei tragen oft die Medien selbst dazu bei, dass dieses System funktioniert; nicht selten nennen sie die Namen bzw. auf das Internet bezogen die sog. Handles der Angreifer.

Die heutigen Angriffe sind jedoch nicht immer zerstörerischer Natur, was die Software oder die Webseiten betrifft, sondern schaden überwiegend dem Image eines Portals und damit auch dem Unternehmen. Ein sog. „Website defacing“ – auch „Web-Graffiti“ genannt – ist ein relativ harmloser Angriff, wenn nicht gleichzeitig wichtige Daten auf dem Server lagen; es werden ein paar Webseiten auf den Webserver eingespielt, die meist eine Nachricht jedweder Art darstellen. Besonders die im E-Commerce Bereich tätigen Unternehmen sind vom Online-Besucher als potentiellen Kunde abhängiger von einem problemlosen Internetauftritt als

xi Im IT-Bereich wird hier auch von „Spoofing“ gesprochen.
xii Der Artemis-Tempel wurde von Herostratus zerstört

Firmen, die ihre Seiten nur zur Information über ihre Produktpalette erstellt haben.

Die jedoch in Mode gekommenen „Denial-of-Service“ (DoS) und „distributed Denial-of-Service“ (dDoS) Angriffe sind um einiges destruktiver, was die bekanntesten DoS Attacken bei *ebay.com*, *dell.com* und *yahoo.com* durch den 15-jährigen Cracker „Mafiaboy“ [Zot00] belegen. Große Webserver sind bei diesem Angriff, der unter 2.1.4 beschrieben wird, in die Knie gegangen; nur durch den Start eines kleines Skriptes, das es frei im Internet gibt. Es ist sehr deutlich zu sehen, wie die neuen Möglichkeiten von örtlicher Unabhängigkeit und der Technique Propagation (siehe Kap. 1.4 auf Seite 15) die „Welt“ verändert haben.

Es scheint sich eine Subkultur von Cracker-Gruppen – wie die Aktionen der Gruppen „PoizonB0x“ oder „World of Hell“ zeigen [Med01] – gebildet zu haben, die jede für sich ihre Besonderheiten und Wertesysteme auslebt. Aufgenommen werden nur Cracker, die schon einige erfolgreiche Attacken vorzuweisen haben. Untereinander konkurrieren diese Gruppen um die Hegemonie, die Erfolgreichsten bzw. Bekanntesten und, insbesondere unter Seinesgleichen, anerkannt zu sein.

Wie nahe sich jedoch die Aktionen der Cracker mit denen der ethischen Hacker, die es grundsätzlich zu unterscheiden gilt, ähneln, zeigt das folgende Beispiel.

Im Online-Shop des großen spanischen Kaufhauses „El Corte Inglés“ fand der spanische Hacker David Alonso Pérez – mit dem Handle „Kamborio“ – eine Sicherheitslücke, die die Webmaster nach mehrmaligen Anfragen nicht behoben [Cri02]. Erst dann ging Kamborio an die Öffentlichkeit, indem er die Startseite des Online-Shops sicherte und eine eigene einbaute, also ein Website Defacing durchführte. Er sieht es als seine moralische Pflicht an, die Öffentlichkeit zu informieren und Druck auf El Corte Inglés auszuüben, bis die Sicherheitslücke geschlossen wurde. Dass die Aktion illegal war, steht außer Frage, doch war sie auch illegitim? Diesem Hacker und seiner Ethik widmete die spanische Tageszeitung „El Mundo“ in ihrer Rubrik „ARIADN@, Cibersociedad“ eine ganze Seite.

1.6 Die juristische Seite

Obwohl theoretisch alle Formen der Kriminalität, wie Betrug oder Diebstahl, auf die Computerwelt übertragbar sind, scheinen es die Behörden schwer zu haben, die Strafverfolgung auch nach dem Prinzip der Verhältnismäßigkeit anzuwenden. So wurde anfangs im Telekommunikationssektor „die Verlängerung eines Telefonkabels härter bestraft als das fahrlässige Auslösen einer atomaren Explosion“ [Kre00, Wau Holland].

Um einen kurzen Überblick über die juristische Lage in Deutschland und der EU sowie den Schwierigkeiten bei der internationalen Verfolgung von Computerkriminalität zu geben, wird die folgende Einteilung vorgenommen:

Unter Punkt 1.6.1 werden die Begriffsdefinitionen in der deutschen Rechtsprechung erklärt [Jae98], um in 1.6.2 auf die Cybercrime Convention des Europarates einzugehen, die zukünftig die Rechtslage in Deutschland beeinflussen wird.

1.6.1 Rechtsprechung in Deutschland

Wer Daten vorsätzlich ändert, macht sich nach §303a StGB der **Datenmanipulation** strafbar und wird unter zwei Jahre mit Freiheitsstrafe oder Geldstrafe bestraft. Schwere Datenmanipulation – also der Veränderung sensibler Daten oder essentieller Programme – gilt als **Computersabotage** und wird nach §303b StGB mit bis zu 5 Jahren Freiheitsstrafe oder mit Geldstrafe geahndet (Abb. 1.4). Sowohl Computersabotage als auch Datenmanipulation sind nur bei vorsätzlicher Tat strafbewehrt. Diese beiden Paragraphen finden je nach Schwere des Schadens auch bei vorsätzlicher Verbreitung von Viren Anwendung. Diese Sabotage wird oft von ehemaligen oder vor Kurzem gekündigten bzw. gefrusteten Mitarbeitern begangen, die sich auf diese Weise rächen wollen. Es gilt also gleichermaßen internen Angriffen, die durch sog. „innere Kündigung“ der Mitarbeiter hervorgerufen werden, vorzubeugen.

Computerbetrug ist in der aktuellen Polizeilichen Kriminalstatistik die führende Position unter denen in der Computerkriminalität zusammengefassten Straftaten; denn hiermit ist der Kreditkarten- und ec-Kartenbetrug (Abb. 1.2) gemeint, der nach §263a StGB mit bis 5 Jahre Freiheitsentzug oder Geldbuße bestraft werden kann. Dieses gilt auch bei Betrugsabsicht.

Das Abhören der Emissionen von abstrahlenden Geräten – vorwiegend Drucker, Monitore und Datenleitungen, aber auch die immer verbreiteteren Wireless LANs (mehr unter 2 auf Seite 27) – stellt den Tatbestand des **unlauteren Wettbewerbs** dar (§17 II UWG). Ist der Täter gleichzeitig Mitarbeiter (was sehr häufig vorkommt), dann findet §17 I UWG Anwendung. Allgemein wird das **Ausspähen von Daten** nach §202a StGB mit bis zu 3 Jahren Freiheitsstrafe oder Geldstrafe bedroht (Abb. 1.5).

Wird mit manipulierten bzw. sabotierten Daten oder mit ausspionierten Informationen ein Unternehmen erpresst, kommt zum Tatbestand der Computersabotage noch die **Erpressung** hinzu; so könnte man sich einen Einbruch in ein

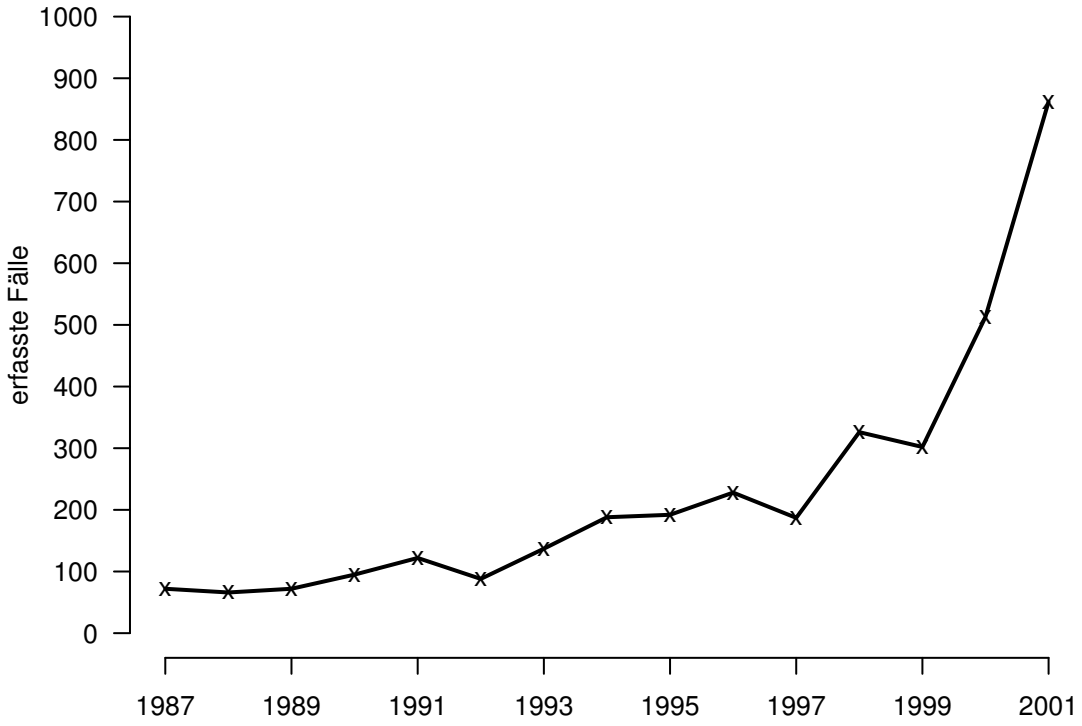

Abbildung 1.4: Computersabotage und Datenveränderung in Deutschland
(Quelle: Polizeiliche Kriminalstatistik des BKA der jeweiligen Jahre [Bun01b])

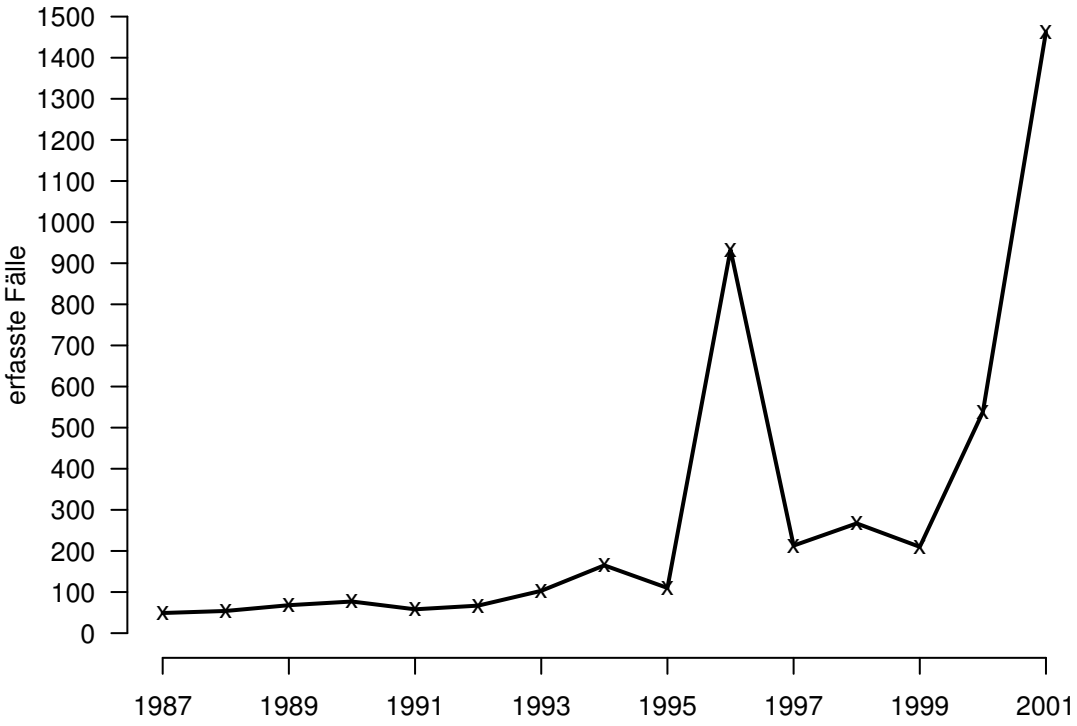

Abbildung 1.5: Ausspähen von Daten in Deutschland
(Quelle: Polizeiliche Kriminalstatistik des BKA der jeweiligen Jahre [Bun01b])

Computersystem vorstellen, bei dem die Kundendatenbank verschlüsselt (Manipulation) und nach Zahlung einer hohen Summe die zur Dekodierung notwendige Passphrase übermittelt wird (Erpressung). Auch ist möglich durch die Androhung der Veröffentlichung der in der Datenbank gespeicherten Informationen ein Unternehmen zu erpressen, dazu ist aber nötig, die Datenbank zu kopieren und das Original zu sabotieren.

Unter **Zeitdiebstahl** wird die widerrechtliche Nutzung der damals noch teuren Rechenzeit gezählt, was immer noch bei Großrechnern vorfallen kann, doch heutzutage eher auf Online-Zeiten, also der privaten Nutzung bei betrieblichen Internetressourcen, übertragen wird. Dieses ist z.Z. strafrechtlich nicht relevant, kann aber zivilrechtliche Folgen in Form von Ersatzansprüchen nach sich ziehen.

1.6.2 Europarat & Cybercrime

Das Ministerkomittee des Europarates ↪**11** verabschiedete am 8.11.2001 die „Convention on Cybercrime“ ↪**12** (ETS-Nr. 185), das am 23.11.2001 von den ersten Staaten unterzeichnet wurde. Der Europarat umfasst 41 Mitgliedsstaaten; die Konvention wurde ebenfalls von den Nicht-Europaratsmitgliedern Südafrika, Kanada, Japan und den USA unterzeichnet. Sie tritt in Kraft, sobald sie von fünf der unterzeichnenden Länder, von denen mindestens drei Mitgliedsstaaten sein müssen, ratifiziert wird (Chapter IV der Konvention, Article 36–48). Als erster Staat hat Albanien am 20.06.2002 die Cybercrime-Konvention in nationales Recht umgesetzt. ↪**13**

In der Präambel wird erwähnt, dass sowohl „ein effektiver Kampf gegen Cybercrime eine wachsende, schnelle und gut funktionierende internationale Kooperation [..] erfordert“ als auch dass eine Kooperation zwischen Staaten und privater Industrie forciert werden müsse.

Inhalt der Konvention ist neben den Begriffsdefinitionen (Chapter I, Article 1) und den durchzuführenden Maßnahmen auf nationaler Ebene (Chapter II, Article 2–23) auch die internationale Kooperation (Chapter III, Article 24–35).

Auf *nationaler Ebene* soll zum einen eine Anpassung des Strafrechts durchgeführt werden (Section 1), was die folgenden Punkte unter Strafe stellt, wenn das noch nicht der Fall ist:

- **Offences against the confidelity, integrity and aviability of computer data and systems:** unerlaubter Zugriff auf Rechnersysteme sowie das Sniffen von

Daten, Störung oder Veränderung der Kommunikation und Computersystemen als auch der Mißbrauch von Geräten und Programmen.

- **Computer-related offences:** Fälschung von Daten sowie Betrug durch Datenveränderung bzw. Störung von Computersystemen.
- **Content-related offences:** Produktion, Vertrieb, Übertragen, Besitzen und Herunterladen von kinderpornografischem Material[xiii],
- **Offences related to infringements of copyright and related rights:** Copyright-Verletzungen im allgemeinen, wie sie insbesondere bei der „World Intellectual Property Organization“ (WIPO) ↪**14** festgelegt wurden,
- **Ancillary liability and sanctions:** Beihilfe und Versuch der oben genannten Taten sind sowohl für natürliche Personen als auch für die Verantwortlichen juristischer Personen strafbewehrt.

Andererseits muss das Prozessrecht (Section 2) geklärt sein:

- **Common Provisions:** Regelt die Verfolgung von Verstößen gegen die Cybercrime Konvention.
- **Expedited preservation of stored computer data:** Fordert die unverzügliche Sicherung und unverfälschte Aufbewahrung von Computerdaten, die den staatlichen Autoritäten zur Verfügung gestellt werden müssen. Ohne richterliche Anordnung können Daten der ISP bis zu 90 Tage gespeichert werden.
- **Production order:** Schaffung einer gesetzlichen Regelung, mit der jede Person verpflichtet werden kann, Computerdaten – wie Kundendaten – herauszugeben.
- **Search and Seizure of stored computer data:** Verabschiedung eines Gesetzes, das den staatlichen Autoritäten ermöglicht, auf alle Computersysteme und Datenspeicher im Lande zuzugreifen. Außerdem können Computersysteme und Datenspeicher beschlagnahmt werden, von denen die staatlichen Autoritäten sogar Daten löschen dürfen. Jede Person, die sensible Daten, beispielsweise mit kryptografischen Verfahren, schützt, kann verpflichtet werden, Informationen für den Zugriff auf diese Daten bereitzustellen.
- **Real-time collection of computer data:** Staatlichen Autoritäten wird es ermöglicht werden, in Echtzeit Kommunikationsdaten und -inhalte zu sammeln.

xiii Xenophobisches und rassistisches Material wird im Zusatzprotokoll „Comitee of Experts on the Criminalisation of Acts of Racist or Xenophobic Nature“ (PC-RX) geregelt, da sich nicht alle Mitgliedsstaaten im Zusammenhang mit der Einschränkung der Meinungsfreiheit in diesem Bereich abfinden konnten.

Der ISP kann verpflichtet werden, diesen Zugang zu gewähren, und wird der Geheimhaltung unterliegen.

In Section 3, der Jurisdiktion, werden die Rechtszuständigkeit sowie die o.a. Verstöße geregelt, wenn sich die Ermittlungen etc. über mehrere Länder erstrecken, d.h. zum Beispiel auch, wenn es um die Auslieferung eines Straftäters geht.

Die *Internationale Kooperation* (Chapter III) umfasst die gegenseitige Hilfe bei der Ermittlung und Sammlung von Beweisen, dessen Daten für einen Zeitraum von mindestens 60 Tage gesichert werden. Verkehrsdaten, die bei einem ISP in einem anderen Mitgliedsstaat anfallen, sollen schnellstmöglich an den Antragsteller übermittelt werden. Jede Vertragspartei muss eine Kontaktstelle schaffen, die jederzeit erreichbar ist und bei der authentifizierte Anfragen per E-Mail oder Fax möglich sein sollen. Sie wird ebenfalls bei der Suche nach Verdächtigen und der Sammlung anderweitiger Beweise tätig werden.

In der Präambel wird ferner über die Problematik, ein gesundes Maß zwischen „law enforcement“ und Menschenrechten zu finden, erwähnt, indem auf den 1950 vom Europarat verabschiedeten Schutz der Menschenrechte und der fundamentalen Freiheit, auf der 1966 von der UNO verabschiedeten „International Convenant on Civil and Political Rights“ und der Konvention von 1981 des Europarates zum Schutze des Individuums und der personenbezogenen Daten verwiesen wird. Ebenso wird auf den Schutz der Privatsphäre und den weltweiten freien Zugang zu Informationen hingewiesen. Später wird in Chapter II, Section 2, Article 15, unter „Conditions and safeguards“ noch einmal auf die Einhaltung der Menschenrechte Bezug genommen.

Inwiefern und wie stark die oben genannten Aspekte zum Schutze der Internetbenutzer wirklich mit einbezogen werden, soll hier nicht ausgeführt werden. Für weitere Informationen sei hier auf die in diesem Bereich agierenden, unabhängigen Nicht-Regierungsorganisationen – wie in der Stellungnahme der „Global Internet Liberation Campaign“ ↪**15** ausgeführt – hingewiesen.

Links

1 http://www.cert.org/
2 http://www.kes.info/_archiv/_onlinesearch/020626-studie.htm
3 http://www.pwcglobal.com/
4 http://www.gocsi.com/

5 http://www.fbi.gov/
6 http://www.nipc.gov/
7 http://www.vogon-international.com/
8 http://tuxedo.org/~esr/jargon/html/entry/hacker.html
9 http://www.riptech.com/
10 http://www.predictive.com/
11 http://www.europarat.de/
12 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
13 http://conventions.coe.int/Treaty/en/searchsig.asp?NT=185
14 http://www.wipo.org/
15 http://www.gilc.org/privacy/coe-letter-1200.html

2 IT-Sicherheitsaspekte

Exkurs: Kompromitierende Emissionen

Die Möglichkeit Abstrahlungen von Geräten aufzufangen und auszuwerten, soll an dieser Stelle nur kurz behandelt werden. Es gibt folgende relevante Arten von kompromitierenden Emissionen:

- **Elektromagnetischen Wellen:** Mit der Abstrahlung sind nicht die nach gesundheitsschädlichen Risiken überprüften Emissionen gemeint, die nach MPR, TCO oder SSI getestet wurden, sondern hierfür gibt es die TEMPEST-Zulassung [Jae98]. Neben der elektromagnetischen Abstrahlung von Monitoren können noch die immer verbreiteteren Funknetzwerke (mehr zu WLAN unter 2.1.5) und die Bluetooth-Kommunikation hinzugezählt werden.
- **Leitungsüberkopplung:** Ein Kabel kann zu einer parallel verlaufenden und von außen erreichbaren Leitung – wie etwa der Stromversorgung – Daten, die in Form von elektrischen Impulsen vorliegen, induzieren, so dass sie aufgezeichnet und ausgewertet werden können. [Jae98]
- **Akustische Abstrahlung:** Durch Analyse von Geräuschen, die die Tastatur oder der Drucker erzeugen, können Rückschlüsse auf die Inhalte getroffen werden. [Jae98]
- **Optische Abstrahlung:** Eine neue Untersuchung [Kuh02] zeigt, wie das schwache Projektionsbild, das CRT-Monitore an eine Wand oder einen Schrank werfen, derart aufbereitet werden kann, dass es fast einem Snapshot des Bildschirmes entspricht.

2.1 IT-Gefahren

2.1.1 Top Ten der Internet-Attacken

Aus der Untersuchung von Internet-Attacken im „Riptech Internet Security Threat Report“ [BY02] wurde eine Top Ten Liste für das zweite Halbjahr 2001 (siehe Tab. 2.1) berechnet, welche bevorzugte Sicherheitslücken darstellt. So wurden 63% der Angriffe durch die Würmer „Code Red“ und „Nimda“ ausgelöst, die sich hauptsächlich der Sicherheitslücken in Microsofts „Internet Information Service“ (IIS) bedienten [BY02].

Aktivität	*Name*	*Beschreibung*
47,8%	Microsoft Index Services ISAPI Overflow Attack	Buffer Overflow in der idq.dll Bibliothek vom IIS, der u.a. von Code Red benutzt wurde.
25,1%	Generic „root.exe“ Request Attack	Code Red II hinterließ eine root.exe Version im infizierten Windows System, die sich der Nimda Wurm zunutze machte.
23,5%	Microsoft IIS Directory Traversal (Unicode) Attack	Probleme mit der Unicode Darstellung in URLs beim IIS. U.a. Nimda nutzte diese Sicherheitslücke.
17,0%	Microsoft IIS Superfluous Decode Attack	Durch doppelte Decodierung einer URL im IIS konnten Befehle ausgeführt werden. (u.a. von Nimda genutzt)
16,5%	Generic „cmd.exe“ Request Attack	cmd.exe vom IIS wird vom Angreifer überprüft, ob Befehle wie „copy“ oder „dir“ ausführbar sind.
5,0%	Scan for 27374/tcp (SubSeven)	Untersucht Port 27374, der üblicherweise von vielen Trojaner- und Backdoor-Programmen, wie SubSeven für Windows, benutzt wird.
3,8%	Scan for vulnerable and/or misconfigured FTP servers	Suche nach falsch konfigurierten oder ungepatchten FTP-Servern (vorwiegend UNIX/Linux), um z.B. beschreibbare Verzeichnisse zu finden, um illegale Inhalte – wie urheberrechtlicht geschützte Dokumente – aufzuspielen.
2,8%	Scans for systems with RPC (tcp) enabled	Suche nach ungepatchten RPC (mountet NFS) in UNIX/Linux-Systemen.
1,3%	Scans for SSH services	Prüft, ob eine SSH Version (vorwiegend UNIX/Linux) installiert ist, die Sicherheitslücken enthält.
1,2%	Scans for LPD services	Prüft, ob eine LPD Version (vorwiegend UNIX/Linux) installiert ist, die Sicherheitslücken enthält.

Tabelle 2.1: Die Top Ten der Attacken im zweiten Halbjahr 2001
(Quelle: Riptech Internet Security Threat Report [BY02])

Aus aktuellen Informationen der Bugtraq-Mailingliste ↪**16** lässt sich jedoch schließen, dass gerade durch die zuletzt bekannt gewordenen Verwundbarkeiten in UNIX/Linux Systemen – wie der Apache-Exploit oder der Buffer Overflow im OpenSSH Dämon – die Reihenfolge sich zu Ungunsten für UNIX/Linux Systeme entwickelt haben könnten, sofern System-Administratoren ihre Rechner nicht gepatcht haben sollten.

2.1.2 Klassifikation von Angriffen

Bei der Art des Angriffs wird grundsätzlich in die Klasse der *„logical attacks“* und der *„flooding attacks“* unterschieden. Die „logical attacks“, mit denen sich 2.1.3 befasst, zielen auf die Sicherheitslücken – wie beispielsweise Buffer Overflows – in Programmen ab, die durch sogenannte „Exploits“ angesteuert werden können und durch schlechte Programmierung entstanden sind. Bei der zweiten Klasse handelt es sich um den Versuch, den Prozessor, den Arbeitsspeicher oder die Netzwerk-Bandbreite zu überlasten, um einen Systemabsturz zu provozieren oder die Verbindung ins Internet zu unterbrechen. Zu dieser Klasse zählen insbesondere die (distributed) Denial-Of-Service Attacken, die unter 2.1.4 behandelt werden. [MVS01]

Laut der Sicherheits-Studie „Internet Risk Impakt Summary“ [Bra02] von Internet Security Systems ↪**17** sind Hybrid-Angriffe, wie sie von den Internet-Würmern Code Red und Nimda verursacht wurden, im Kommen und finden meist von unsicheren privaten Windows-Rechnern aus statt.

2.1.3 Exploits & Buffer Overflows

Buffer Overflows, die zu den „logical attacks“ gezählt werden, sind eine der verbreitesten Sicherheitslücken, die sich Cracker-Tools – sogenannte „Exploits“ – zunutze machen. Sie entstehen durch Programmiersprachen, die die vom Programmierer definierten Zeichenkettenlängen nicht überprüfen, so dass durch Überladen des Strings der Speicher nach der Zeichenkette mit ausführbarem Code überschrieben werden kann, und Programmierer, die nicht alle diese Sicherheitsabfragen eingebaut haben. Bei der Programmiersprache „Perl“ ist so eine Überprüfung schon von Compilerseite implementiert und es empfiehlt sich derartige Programmiersprachen zu verwenden.

Da bei Open-Source Programmen jeder den Quellcode lesen und überprüfen kann, ist es schneller möglich Patches zu entwickeln. Außerdem gibt es mehr Sicherheitsexperten, die sich den Source-Code anschauen, als es bei proprietä-

ren Betriebssystemen, wie Microsoft Windows, der Fall ist. Ein aufwendiges Re-Engineering, was Sicherheitslücken zu Tage fördern könnte, ist dort verboten. Wie lange es bei Microsoft dauert, Sicherheitslücken im InternetExplorer zu schließen, zeigt diese Liste ↪**18** mit ungepatchten Sicherheitslöchern.

2.1.4 (Distributed) Denial-Of-Service Angriffe

An erster Stelle stehen laut Computer Crime and Security Survey 2002 von CSI und FBI [Pow02] (siehe 1.2.3 auf Seite 11) Vandalismus und Denial-of-Service Angriffe (DoS), letztere können ebenfalls in die Kategorie „Vandalismus“ eingeordnet werden.

Es gibt **zwei** unterschiedliche Ziele für „flooding attacks“: Einmal kann versucht werden, die begrenzte **Bandbreite** oder „packet processing rate“ von Routern oder NICs mit einer großen Anzahl kleinerer Paketen zu überladen. Auf der anderen Seite ist es möglich, die **CPU** des anzugreifenden Computers zu überlasten, z.B. durch das Versenden von TCP SYN-Paketen, auf die der Rechner als erstes seine bestehenden Verbindungen durchsuchen und folglich (bei Nichtauffinden) begrenzte Datenstrukturen für die neue Verbindung allokieren muss. Die sehr häufig vorkommenden Angriffe mit TCP SYN-Paketen werden deshalb auch als „SYN Flood“-Attacken bezeichnet. [MVS01]

Ein DoS-Angriff – wie oben beschrieben – hat aber nur eine begrenzte Senderate auf der Seite des Angreifers, weshalb sich distributed DoS (dDoS) Attacken etabliert haben. Dabei werden mit kleinen Attack-Dämonen kompromitierte Hosts benutzt, um einen verteilten DoS Angriff zu starten. Eine der neuesten Varianten ist die Benutzung von File-Sharing Programmen, wie Gnutella, als Reflektoren für dDoS Pakete, was eine neue Dimension von dDoS Angriffen darstellt [Pax01].

Nach einer Untersuchung der Universität von Kalifornien von dDoS Attacken im Zeitraum von drei Wochen mit einer „Backscatter Analysis“ [MVS01], bei der 12.805 Angriffe auf über 5.000 Zielrechner analysiert wurden, waren erstaunlicherweise die häufigsten Opfer Privatrechner und nicht wie vermutet kommerzielle Ziele. Wenn Unternehmen angegriffen wurden, waren es kleine und mittelständische Unternehmen. Die Backscatter Analysis beruht auf der Auswertung der von dDoS Programmen – wie Stacheldraht, TFN oder Trinoo – zufällig generierten Absenderadresse[i], anhand derer Angriffe festgestellt und Rückschlüsse gezogen

i Der Angreifer übermittelt natürlich nicht seine IP-Adresse, sondern erzeugt falsche Absender-

werden können.

Eine interessante und ausführliche Analyse des distributed DoS Attacks des 13-jährigen Crackers „Wicked“ mithilfe des Trojanischen Pferdes „SubSeven“, das Microsoft Windows-Systeme befällt und in IRC-Channels auf Befehle lauscht oder Informationen über Zugangsdaten postet, gibt Steve Gibson in „The Strange Tale of the Denial of Service Attacks against GRC.COM“ [Gib02].

2.1.5 Abhören von IP-basierter Kommunikation

Packet Sniffer

Packet Sniffer, wie Aldebaran, `tcpdump` oder Ethereal, bauen alle auf der libpcap ↪**19** Bibliothek auf, die unter Windows als WinPcap ↪**20** oder in Java als JPcap ↪**21** verfügbar ist. Sie ermöglicht es, den Datenverkehr zu belauschen und Pakete durch Filterregeln herauszusuchen. Mögliche Ziele wären beispielsweise die Suche nach Logins und Passphrasen oder Kreditkarteninformationen. Diese Aktionen können jedoch nur erfolgversprechend sein, wenn die Kommunikationdaten nicht verschlüsselt werden, der Inhalt der Pakete also „plain“ übertragen wird.

Selbst wenn der Sniffer am Ende eines *Switches* hängt, braucht er nicht gleich den Netzknoten zu erobern: Durch MAC-Spoofing mit Tools wie `arp0c` ↪**22** und `dsniff` ↪**23** oder Random MAC-Flooding mit `angst` ↪**24** werden Switches verwirrt, sodass sie die Pakete wie bei Hubs an alle ihre Ports senden – auch an den, wo der Angreifer sitzt. [Iac02]

Um selber nicht durch abgehende Pakete wahrgenommen zu werden, gibt es für Linux Kernel-Patches, wie dem Stealth-Patch ↪**25**, der das Senden von Paketen auf Kernel-Ebene unterbindet.

Es mag hier vielleicht den Anschein gegeben haben, dass Packet Sniffer nur von Cracker und nur zu böswilligen Zwecken benutzt werden. Dies ist nicht der Fall. Zur Analyse des Netzwerkverkehrs ist ein Sniffer für System-Administratoren essentiell.

---

adressen, was beim IP-Protokoll ohne weiteres möglich ist und unter dem Begriff „Spoofing“ läuft.

Wireless LAN

Wie bei den anderen Internet-Protokollen stand auch bei der Entwicklung der nach IEEE 802.11b definierten Funknetzwerke, auch Wireless LAN (WLAN) genannt, die Bandbreite und weniger die Sicherheit im Mittelpunkt. Das bedeutet, dass die Sicherheit in Form von IPSec bei IP-basierter Kommunikation oder mit dem „Wired Equivalent Protocol“ (WEP) für WLANs nachträglich aufgesetzt werde musste [Gas02, Kin01]. Hinzukommt beim WLAN noch, dass im WEP-Protokoll der Verschlüsselungsalgorithmus „RC4“ vorgeschrieben ist, der unlängst durch Cipher-Text Angriffe geknackt werden konnte [FMS01].

Die meisten AccessPoints sind jedoch ungenügend geschützt, d.h. systemfremde Rechner können sich problemlos anmelden und Ressourcen mitnutzen [VB01, Cox01]. Gerade in sensiblen Bereichen, wie dem Gesundheitswesen, besteht die Gefahr, dass Patientendaten verändert werden könnten. Beispiele von offenen Netzen gibt es genügend (siehe SternOnline-Artikel ↪**26**).

Einer der bekannteren Sniffer für WLANs ist AirSnort ↪**27**, der ebenfalls einen Cipher-Text Angriff auf die gesammelten Pakete durchführt und damit die Verschlüsselungskeys bekommt.

Voice-over-IP

Nicht nur als Haustelefon scheint sich in Unternehmen immer mehr das Telefonieren über IP-basierte Netze (Voice-over-IP) – wie Intra- oder Internet – auszubreiten, da neben dem finanziellen Vorteil die Verbindung sowohl für Audio- als auch für Bild- und Videodaten genutzt werden könnte. Der große Nachteil ist die mit trivialen Methoden durchzuführende Abhörmaßnahme, falls die Daten unverschlüsselt übertragen werden:

Aldebaran ↪**28** fertigt, genauso wie Ethereal ↪**29** und `tcpdump` ↪**30**, Kopien des Datenstroms an, kann diese aber zusätzlich als UDP-Datagramme an einen anderen Host (des Lauschers) weiterleiten, wo echtzeitorientierte Programme ebenfalls das UDP-Protokoll verwenden. Aus den Header-Informationen ist leicht die Codierung zu entnehmen, um die Daten wiederzugeben. [Iac02]

Das unter 2.2.5 beschriebene IPSec und dem relativ neuen Secure Real-Time Transport Protocol (SRTP), der zur Zeit in der IETF diskutiert wird, schaffen Abhilfe, sind aber mit intensiver Admin–Arbeit verbunden. Das SRTP beinhaltet neben den üblichen Vertraulichkeits–, Authentifikations– und Integritätsdiensten auch Schutz vor Replay-Attacken. [Iac02]

2.2 Sicherheit aufbauen

Entgegen der Meinung von über 300 von der Hurwitz Group ↪**31** befragten Computerexperten, die sich für eine sofortige Veröffentlichung von Sicherheitslücken, der sogenannten „full disclosure“, aussprachen, ist Microsoft der Auffassung, dass erst nach einem Zeitraum von über 30 Tagen die Veröffentlichung vorgenommen werden sollte, damit rechtzeitig Sicherheits-Patches entwickelt werden können. [Sch02]

Sicherheitsmodelle

Computersicherheit setzt an dem Punkte an, wenn Dateirechte, Zugriffrechte auf Datenbanken etc. vergeben werden, um verschiedene Sicherheitsebenen zu schaffen. So sind beispielsweise Benutzerrechte in Windows 9x Systemen nicht vorhanden. Windows XP wurde zwar für einen Multiuser-Betrieb gerüstet, doch ist der Standardbenutzer gleichzeitig Administrator. Das stellt ein unzureichendes Sicherheitskonzept dar, da Sicherheit dadurch zustande kommen soll, dass einem neuen Benutzer erst standardmäßig alle Rechte gegeben werden, um sie nachher auf ein gesundes Maß zu reduzieren. UNIX/ Linux-Systeme gehen von der anderen Seite das Problem an: Ein neuer Benutzer hat so wenig Rechte wie möglich, nach und nach können ihm neue zugewiesen werden.

Einen kurzen Überblick über Sicherheitsmodelle für Betriebssysteme und Datenbanken soll hier gegeben werden [Fug96]:

Betriebssystemmodelle:

- **Bell-LaPadula-Modell:** Zum Schutz wird jedem Betriebssystemobjekt (Dateien,..) bzw. -subject (Benutzer, Prozesse, ..) einer Sicherheitsstufe zugeordnet; ob Sicherheitseigenschaften eingehalten werden, wird über Sicherheitsaxiome überprüft.
- **Biba-Integrity-Modell:** Wie der Name schon sagt, geht es beim Biba-Integrity-Modell an erster Stelle um die Aufrechterhaltung der Integrität. Immer wenn Informationen verändert werden, wird die Integrität kontolliert, zum Beispiel mithilfe von einer „access controll list“ (ACL).
- **Dion-Protection-Modell:** Komplexer und etwas weiterentwickelter ist das Dion-Protection-Modell, da es sowohl die Integrität als auch die Vertraulichkeit vereint; es kommt aber durch die Kombination von Sicherheits- und Integritätsstufen zu höherer Komplexität.

DBMS-Modelle:

- **MITRE-Modell:** Das vom MITRE Unternehmen entwickelte Modell für relationale Datenbanken schützt vor unberechtigtem Zugriff mithilfe von ACL, „Default Security Level“ (DSL), „Implicit Security Level“ (ISL) sowie Sicherheitsaxiomen.
- **I.P. Sharp-Modell:** Dieses Modell wurde ebenfalls für relationale Datenbanken konzipiert. Es weist jeder Relation eine Schutzstufe zu, die auch eine Integritätsstufe enthält, und überprüft mit Axiomen die Korrektheit.

Allgemeine Modelle:

- **Zugriffsmatrix-Modell:** Beim Zugriffsmatrix-Modell wird eine zweidimensionale Matrix anstelle von Sicherheitsaxiomen definiert, die bei Zugriff befragt wird.
- **Take-grant-Modell:** Hier wird auch mit einer Zugriffsmatrix Rechte festgelegt, doch mit dem Unterschied, dass sowohl eine Vererbung der Recht auf andere Objekte möglich ist, als auch dass Axiome definiert werden können.

2.2.1 CERT

Das erste „Computer Emergency Response Team“ (CERT) wurde Ende 1988 an der Carnegie Mellon University in Pittsburgh aufgrund des ersten „Internet“-Wurmes, der den Vorgänger des Internet, das Arpanet, mithilfe von Sicherheitslücken in den Programmen „finger“ und „sendmail“ UNIX-Systeme infizierte, gegründet. Weltweit gab es gleiche Anstrengungen, die in Deutschland zu den drei CERTs, CERT-Bund ↪**32** des BSI (früher BSI-CERT, 1993), DFN-CERT ↪**33** des Deutschen Forschungsnetzes e.V. (1993) und RUS-CERT ↪**34** des Rechenzentrums der Universität Stuttgart, führten.

Viele CERTs sind über das CERT/Coordination Center ↪**35** in Pittsburgh zusammengeschlossen, das regelmäßig Sicherheits-Bulletins und Alarmierungen herausgibt [Fox02]. Eine Grafik der dem CERT/CC gemeldeten Vorfälle befindet sich in Abb. 1.1 auf Seite 2.

Informationen über sicherheitsrelevante Themen sind auch beim „Forum of Incident Response and Security Teams“ ↪**36** (FIRST), das ebenfalls ein Zusammenschluss von CERTs darstellt und das Fachkonferenzen und Workshops anbietet, sowie dem „System Administration, Networking and Security Institute“ ↪**37** (SANS) oder über Mailing-Listen, wie „bugtraq“ ↪**38** zu finden.

2.2.2 Firewalls und Intrusion Detection Systeme

Firewalls zählen heutzutage zu den verbreitesten Schutzmechanismen gegen externe Gefahren, doch schützen sie nur, wenn sie richtig administriert werden, da Sicherheit – wie anfangs erwähnt (1.1.1) – einen Prozess darstellt, der regelmäßige Wartung erfordert. Firewalls funktionieren über Filterregeln (vgl. `ipchains` bzw. `iptables` bei Linux), die bestimmte Pakete auf bestimmte Ports zulassen (accept), verweigern (deny) oder zurückweisen (reject) [Tox01, S. 407].

Intrusion Detection Systeme (IDS) ergänzen Firewalls mit einer Analyse der Log-Dateien und des Datenverkehrs auf Anomalien, wie beispielsweise auf Portscans, die protokolliert werden und je nach Grad der Sicherheitsverletzung Informationen an den Administrator schicken oder selbständig vordefinierte Maßnahmen, wie das umstrittene[ii] (zeitlich begrenzte) Blockieren einiger IPs oder auffälliger Class-[A | B | C]-Netzwerke, ergreifen. [Tox01]

Intrusion Detection Systeme werden nur von einem Drittel der Unternehmen verwendet, die in der KES/KPMG Sicherheitsstudie befragt wurden [SH02]. Dabei ist es auch für kleinere und mittelständische Unternehmen oder Privatpersonen nicht schwierig eine Firewall mit IDS einzurichten, da freie Projekte wie „Smoothwall“ ↪**39** existieren: Smoothwall maskiert die dahinterliegenden (Windows-) Rechner und basiert auf einem Linux-System mit VPN Unterstützung und Administration über ein Web-Interface.

2.2.3 Security Scanner

Security Scanner, wie SAINT ↪**40** oder Nessus ↪**41**, untersuchen mit den gleichen Methoden und Mitteln wie ein Cracker nach Sicherheitslücken und Einstiegspunkten ins System, beispielsweise führen sie auf der Suche nach offenen Ports Portscans durch. Das Ergebnis gibt dem Administrator Informationen, wie er sein System sicherer gestalten kann.

Da Security Scanner auch von Crackern gegen einen beliebigen Host genutzt werden können, ist eine Diskussion entbrannt, inwiefern solche Programme überhaupt verfügbar gemacht werden dürfen: In der ersten Version der europäischen Cybercrime Convention sollten „Hacker-Tools“ noch verboten werden. Dieser Passus wurde in neueren Versionen gestrichen.

---

ii Umstritten sind IP-Sperren, weil die Herkunft eines IP-Paketes nicht sicher bestimmt werden kann, also ein IP-Spoofing möglich wäre und unschuldige Rechner blockieren könnte. [Sch01]

Ohne diese Werkzeuge ist es für System-Administratoren um einiges schwieriger, Sicherheitslücken im eigenen System auszumachen. Deshalb sind sich Sicherheitsexperten einig, dass Security Scanner verfügbar sein müssen.

2.2.4 Starke Kryptografie

Starke Verschlüsselungsalgorithmen sind die Grundlage für abhörsichere Kommunikation. Zusammen mit One-Way-Hash-Funktionen [Sch00] lassen sich Daten, z.B. im E-Mail Verkehr oder Dateien auf der Festplatte, vor Unbefugten übertragen und lagern. Bisher nutzen 44% der Unternehmen, die den Schlüssel des Kommunikationspartners besitzen, Verschlüsselung für sensitive Nachrichten. Phil Zimmermanns Pretty Good Privacy (PGP) ↪**42** wird dabei doppelt so häufig wie S/MIME verwendet [SH02]. Ein freies und vom deutschen Wirtschaftsministerium finanziell unterstütztes Verschlüsselungsprogramm ist GnuPG ↪**43**.

DES (Data Encryption Standard) [Fox00] war lange Zeit der übliche Verschlüsselungsstandard, der den 1975 von IBM entwickelten „Lucifer“ Algorithmus verwendete, der leider auf 56-bit begrenzt wurde. 1997 wurde zur Definition des neuen „Advanced Encryption Standard“ (AES) ↪**44** ein Wettbewerb vom NIST gestartet, bei dem Kryptografen ihre Ideen vorstellen sollten. Der „Rijndael“-Algorithmus gewann vor Bruce Schneiers „Twofish“ und wurde so zum DES-Nachfolger [LW00]. Er unterstützt Chiffren mit 128-bit Blockgröße und Schlüssellängen von 128, 192 und 256-bit.

Im Crypto-Gram-Newsletter ↪**45** vom 15. September 2002 berichtet Bruce Schneier, dass AES und Serpent möglicherweise knackbar sind. Die zwei veröffentlichten Angriffe von Courtois/Pieprzyk und Fuller/Millan basieren auf innovativen mathematischen Verfahren, die die Komplexität des Algorithmus verringern könnten. Beunruhigen wollte Schneier bislang nicht, da es sich bisher noch um „plain-text“-Angriffe handelte, die aber besser als Brute-Force-Angriffe gegen AES und Serpent funktionieren.

2.2.5 IPSec

IP Security – kurz IPSec – ist eine Erweiterung des IP-Protokolls um Sicherheitsaspekte, mit denen sowohl die Integrität und Authentizität also auch eine Verschlüsselung der Pakete gewährleistet wird; ebenso bietet IPSec die Möglichkeit, Replay-Attacken zu erkennen und abzuwehren. Es wurden die zwei neuen Protokolle *Authentication Header* (AH) und *Encapsulated Security Payload* (ESP) hinzugefügt. Der AH verwendet die One-Way-Hash Funktionen SHA1 und MD5, um über die

Prüfsumme die Authentizität sowie Integrität eines Paketes zu verifizieren. ESP bildet die Verschlüsselungskomponente.

Die beiden neuen protokolltransparenten Betriebsarten von IPSec sind der Tunnel-Modus, der ähnlich dem SSH-Tunnel funktioniert, und der Transport-Modus, bei dem der Inhalt des Paketes auf Integrität und Authentizität überprüft wird.

Eine Implementierung für IPSec muss die oben genannten Hash-Routinen sowie folgende Krypto-Verfahren enthalten: AES, Blowfish, DES, 3DES, DFC, IDEA, MARS, RC5, RC6, SERPENT, TWOFISH und eine NULL-Verschlüsselung. Für den Transport-Modus heisst das, dass der ESP die NULL-Verschlüsselung verwendet, also keine Verschlüsselung. Anwendung findet IPSec bei Virtual Private Networks (VPN).

Eine mögliche modulare Umsetzung für Linux sieht das Paper [CMM+02] von Studenten der Univerität Karlsruhe vor: Sie benutzen die International Crypto-API ↪**46**, die alle nötigen Hash- und Verschlüsselungsverfahren beinhaltet, und bearbeiten die IP-Pakete auf netfilter-Ebene.

2.3 Sicherheitsstandards und -zertifizierung

Durch die steigende Verbreitung der neuen Kommunikationsmittel – wie E-Mail, Online-Banking oder E-Commerce –, die sensible Daten transportieren, müssen mögliche Risiken minimiert und das Vertrauen in diese Anwendungen aumentiert werden, um Integrität und Vertraulichkeit zu gewährleisten. Eine Zertifizierung nach internationalen Standards kann die Sicherheitseigenschaften der IT-Produkte bescheinigen, eine bestimmte Sicherheitsstufe zu erfüllen. Methoden der Evaluation helfen den Sicherheitsgrad festzustellen und machen das Ergebnis durch die Standardisierung weltweit vergleichbar [BSI02b].

Insbesondere kommen diese Zertifizierungen bei IT-Produkten vor, bei denen es gesetzlich vorgeschrieben ist, wie etwa bei Produkten zur digitalen Signatur, die nach dem Signaturgesetz (SigG) [Bun01a] in Deutschland Anwendung finden sollen. Ebenfalls sind Zertifizierungen bei Smartcards, Kartenlesegeräten, Betriebssystemen, DBMS etc. sinnvoll.

Weniger als 60% der Unternehmen haben eine der bewährten Computersicherheitspolicen, stellt Vogon International [SCJ00] fest.

Unter Kap. 2.3.1 werden die in Deutschland am weitesten verbreiteten Standards, ITSEC und Common Criteria, vorgestellt. Ein jüngerer Standard ist der vom British Standard Institute (BSi) zertifizierte BSi 7799, der auch als ISO 17799 standardisiert wurde und auf den hier nicht eingegangen wird. Er beschreibt die Anforderungen an ein „Information Security Management System“ (ISMS), das größtenteils im E-Commerce Bereich Anwendung findet, und basiert auf generischen Verfahren. Er wurde bis Anfang 2002 nur einmal[iii] in Deutschland vergeben.

2.3.1 Common Criteria & ITSEC

Historische Entwicklung

Die *Common Criteria* ↪**48** stellt die systematische Evaluierung mithilfe von veröffentlichten Kriterien, wie etwa Schutzprofilen, seit Anfang der 1980er dar. Zu dieser Zeit entwickelte das US-amerikanische Verteidigungsministerium das sogenannte „Orange Book“ ↪**49** [Str91, S. 78], das unter dem Namen „Trusted Computer Systems Evaluation Criteria“ (TCSEC) veröffentlicht wurde. In Europa entstanden 1991 die auf die TCSEC aufbauenden „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik“ (Information Technology Security Evaluation Criteria), kurz *ITSEC*, das die verschiedenen europäischen Evaluationskriterien – in Deutschland waren das die „IT-Sicherheitskriterien“ – harmonisieren sollte. [Mac02]

Die Version 2.1 vom August 1999 der Common Criteria (CC) wurde Anfang Dezember 1999 von der Internationalen Standardisierungsorganisation ↪**50** als ISO/IEC 15408 unter Beteiligung von vielen Ländern[iv] veröffentlicht. Durch diese Standardisierung wurden die nationalen Evaluationskriterien aus Deutschland (ITSEC), den USA (TCSEC und FC) und Kanada (CTCPEC) in den CC in Einklang gebracht, was nun weltweit vergleichbare Sicherheitszertifikate und Evaluationsergebnisse möglich macht. Die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) ↪**51** lizenzierten Prüfstellen können dann für Deutschland IT-Produkte oder -Systeme (auch Hardware) nach dem CC-Standard zertifizieren.

iii Das deutsche Unternehmen @sec Security GmbH ↪**47** zertifizierte Vodafone TeleCommerce als erstes deutsches Unternehmen nach BSi 7799. [ats02]

iv mit Beteiligung von folgenden Instituten (Ländern): BSI (Deutschland), DCSSI (Frankreich), CESG (Großbrittanien), NLNCSA (Niederlande), CSE (Kanada), NIST (USA) und NSA (USA)

Das CC-Modell

Die CC definiert detailliert exakte Prüfvorgaben für IT-Produkte und -Systeme. Um von bestimmten Produkttypen unabhängige Richtlinien zum Evaluieren aufstellen zu können, werden *Schutzprofile* definiert, die mithilfe von produktspezifischen *Sicherheitsvorgaben* auf ein IT-Produkt angepasst werden.

Der **erste** von drei Teile der CC stellt das allgemeine Modell vor, in dem die hierarchischen und auf Wunsch ergänzbaren Vertrauenswürdigkeitsstufen, die *„Evaluation Assurance Level"* (EAL), vorgestellt werden. Diese sollen das Vertrauen eines Benutzers in die Sicherheitsmaßnahmen ausdrücken und werden durch Analyse von Schwachstellen, wie beispielsweise durch Penetrationstests, von einem erfahrenen Evaluator überprüft, ob die bestehenden Sicherheitsfunktionen einem Angriff auf diesem Niveau (EAL) Stand halten würden.

Bei den Schutzprofilen (Protection Profiles) muss als erstes der konkrete *Evaluationsgegenstand* (EVG) festgelegt werden, auf den die definierten Sicherheitsziele mit verschiedenartige Bedrohungen überprüft werden. Anders als bei ITSEC können bei den CC nicht nur die IT-Hersteller und Antragsteller, sondern auch der IT-Anwender die Schutzprofile formulieren. Ein Schutzprofil setzt sich aus EVG-Beschreibung und Sicherheitsumgebung, Formulierung der Sicherheitsziele sowie der IT-Sicherheitsanforderungen zusammen. Die Sicherheitsvorgaben müssen abhängig von den gegebenen EVG festgelegt werden.

Im **zweiten** Teil werden Funktionalitätsanforderungen beschrieben, die bei der Formulierung der Schutzprofile und Sicherheitsvorgaben Anwendung finden. Sie sind in Klassen, Familien und Komponenten geordnet, wobei eine Dependenz zwischen den Komponenten besteht; das bedeutet, bei der Wahl einer Komponente müssen die Abhängigkeiten mit anderen Komponenten berücksichtigen werden. Die Wahl der Komponenten beeinflusst beispielsweise die Stufe der Protokollierung (minimale, einfache oder detaillierte).

Sicherheitsanforderungen zur Vertrauenswürdigkeit werden im **dritten** Teil der CC ausgeführt und liefern die Kriterien zur Evaluierung von Schutzprofilen und Sicherheitsvorgaben. Letztere werden zuerst ohne den Einfluss des EVG evaluiert. Vertrauenswürdigkeitskomponenten bilden nach sinnvollem Zusammenfügen eine *Evaluationsstufe für die Vertrauenwürdigkeit* (EAL), die wiederum in Gruppen gefasst werden. Die Prüftiefe der Evaluation besteht aus sieben Stufen, die in Anlehnung an die sechs E-Stufen von ITSEC EAL1, EAL2 (≙E1) .. EAL7 (≙E6) lauten. EAL1 bildet eine niedrigere Stufe als sie in ITSEC existierte; sie soll

neue Unternehmen locken, sich zertifizieren zu lassen.[v] Sollte ein EVG höheren Anforderungen als die vorgegebenen gerecht werden, kann das durch Hinzufügen schärferer Anforderungen ausgedrückt werden.

Das Unternehmen @sec hält jedoch die Common Criteria als so komplex, dass Unternehmen entmutigt werden können, ihre Produkte zu zertifizieren [ats02].

Links

16 http://online.securityfocus.com/archive/1
17 http://www.iss.net/
18 http://www.pivx.com/larholm/unpatched/
19 http://ee.lbl.gov/
20 http://netgroup-serv.polito.it/winpcap/
21 http://www.goto.info.waseda.ac.jp/~fujii/jpcap/
22 http://www.phenoelit.de/arpoc/
23 http://www.monkey.org/~dugsong/dsniff/
24 http://angst.sourceforge.net/
25 http://www.energymech.net/madcamel/fm/
26 http://www.stern.de/computer-netze/readme/pflichtlektuere/artikel/?id=157473
27 http://airsnort.shmoo.com/
28 http://www.rogola.3d.pl/
29 http://www.ethereal.com/
30 http://www.tcpdump.org/
31 http://www.hurwitz.com/
32 http://www.bsi.de/certbund/
33 http://www.dfn-cert.de/
34 http://cert.uni-stuttgart.de/
35 http://www.cert.org/
36 http://www.first.org/
37 http://www.sans.org/
38 http://online.securityfocus.com/archive/1
39 http://www.smoothwall.org/
40 http://www.wwdsi.com/products/saint_engine.html
41 http://www.nessus.org/
42 http://www.pgpi.net/

---

v „Sun Solaris 8 with AdminSuite v3.0.1“ bekam im November 2000 das Ergebnis EAL4, „Microsoft Windows NT Workstation and Server Version 4.0“ im März 1999 die Stufe E3 (≙EAL4) zertifiziert [BSI02a].

43 http://www.gnupg.org/
44 http://csrc.nist.gov/encryption/aes/
45 http://www.counterpane.com/crypto-gram.html
46 http://sourceforge.net/projects/cryptoapi
47 http://www.atsec.com/
48 http://www.commoncriteria.org/
49 http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html
50 http://www.iso.org/
51 http://www.bsi.bund.de/

3 Unternehmenskultur & Identifikation

Im vorigen Kapitel wurden die Gefahren, die ein Unternehmen von der technischen Seite her bedrohen, und die Möglichkeiten, sie zu kontrollieren, diskutiert. In diesem Kapitel soll der menschliche Faktor, der bisher nur als Verursacher von Programmierfehlern oder als Angreifer mit technischem Werkzeug in die Arbeit eingegangen war, untersucht werden.

Wie sieht es also mit den eigenen Mitarbeitern aus? Um dieses Thema besser fassen zu können, wird sich der Unternehmenskulturen und ihrer Auswirkungen bedient. Dazu muss erst einmal der Begriff der Unternehmenskultur (3.1) mit möglichen Klassifikationen (3.2), die eine Bewertung möglich machen, geklärt sein. Auch die Bewertungsstrategie muss einer genauen Betrachtung unterworfen werden, da bei einem derart komplexen Gebiet keine einfachen Sieger oder Verlierer existieren. Mit ihnen wird sich im Unterkapitel „Unternehmenssicherheit“ (3.3) auseinandergesetzt.

3.1 Begriff der Unternehmenskultur

Allgemeine Kulturdefinitionen

Der in der Ethnologie gewachsene Begriff der Kultur beschreibt nach Kluckhohn/ Strodtbeck (1961) aus [Sch99, S. 437] die „besonderen, historisch gewachsenen und zu einer komplexen Gestalt geronnenen Merkmale von Volksgruppen“, unter denen man sich sowohl Wert- und Denkmuster als auch Symbolsysteme vorstellt.

Geert Hofstede [Hof01] definiert den Begriff der Kultur als „mentale Programmierung“, die wir durch unser soziales Umfeld, in dem wir aufwachsen, erwerben und die sich durch Denk-, Fühl- und Handlungsmuster im Kopf manifestiert. Kultur ist die „kollektive Programmierung des Geistes, die die Mitglieder einer Gruppe oder Kategorie von Menschen von einer anderen unterscheidet“ [Hof01].

Die mentale Programmierung ist erlernt und wird nicht mit den Genen weitergegeben; nach Hofstede existieren drei Ebenen (Abb. 3.1), die ein Individuum prägen: Die Basis bildet die menschliche Natur, die universell für jeden Menschen gilt und die vererbt wird. Darüber steht die Kultur, die gruppen- oder kategorienspezifisch erlernt wird (Sozialisation). Als oberste Ebene steht die Persönlichkeit, die mit dem Erlernten und Erlebten das Individuum ausmacht; was aber nicht

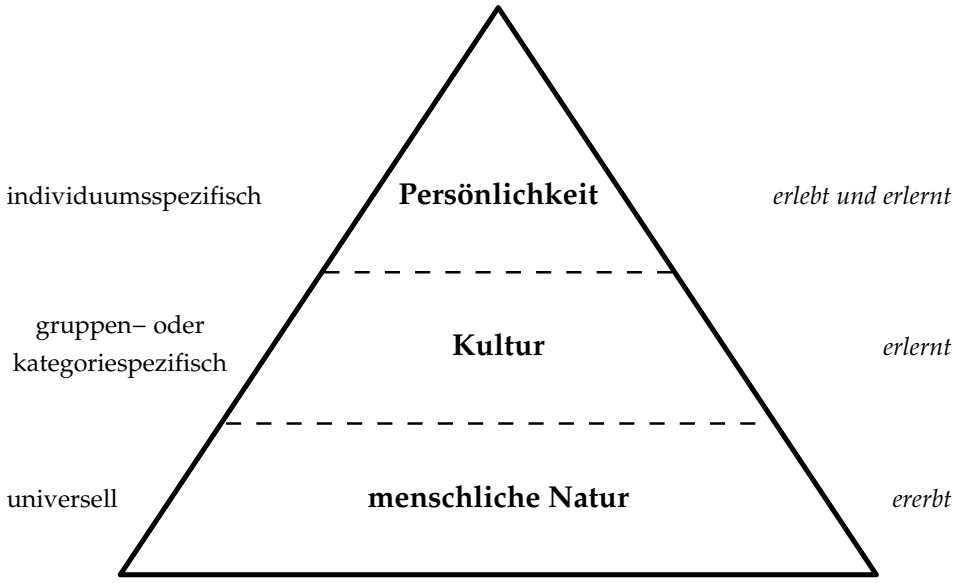

Abbildung 3.1: Drei Ebenen der Einzigartigkeit in der mentalen Programmierung *(Quelle: Geert Hofstede [Hof01])*

bedeutet, dass eine einmal erlernte Kultur nicht wieder partiell ablegbar wäre. Das Verwerfen einer Kultur ist nur um einiges schwieriger als sie (das erste Mal) zu erlernen. Die erlernbaren Eigenschaften können sich also ändern bzw. können beeinflusst werden [Hof01].

Hofstede beschäftigt sich zwar mit nationalen Kulturen, doch sieht er den Begriff der Kultur als nicht an territoriale Grenzen gebunden an, wie sich schon an seiner Definition von Kultur zeigt.

3.1.1 Corporate Culture

Zwischen Unternehmenskulturen und „nationalen“ Kulturen muss deutlich differenziert werden: Sie sind verschiedene Phänomene. Während „nationale“ Kulturen länger historisch gewachsen sind und der Sozialisationsprozess von Kindheit an durchlaufen wird, sind Unternehmenskulturen nur bedingt an nationale Kulturen gebunden (siehe hierzu IRIC-Studie von Unternehmenskulturen in den Niederlanden und Dänemark [Hof01]).

Analog zu seiner allgemeinen Kulturdefinition versteht Hofstede unter einer Unternehmenskultur „die kollektive Programmierung des Geistes, die die Mitglieder einer Organisation von einer anderen unterscheidet“ [Hof01].

Die Organisationskultur (organizational culture) entstand in den 1960er Jahre als Beschreibung für das Klima in einem Unternehmen. Später, in den 1970er Jahren, bildete sich der Ausdruck Unternehmenskultur (corporate culture), der durch Deal/ Kennedy geprägt wurde. Beide Begriffe werden aber synonym gebraucht [Sch99]; hier wird der Begriff der Unternehmenskultur verwendet.

3.1.2 Kernelemente

Schreyögg [Sch99] beschreibt als Kernelemente einer Unternehmenskultur die folgenden sechs, am häufigsten in der Literatur genannten Punkte:

- **implizit:** Durch „gemeinsam geteilte Überzeugungen" prägen Unternehmenskulturen das Selbstverständnis der Unternehmen (Bate, 1984). Sie werden als selbstverständlich angesehen, wobei es oft an einer Selbstreflexion mangelt.
- **kollektiv:** Unternehmenskultur ist ein „kollektives Phänomen", das das Agieren des Einzelnen durch gemeinsame Werte und Orientierungen bestimmt.
- **konzeptionell:** Um sich in einer komplexen Welt Orientierung verschaffen zu können, gibt die Unternehmenskultur den Beteiligten Orientierung und Sinn. Sie stellt dabei eine „konzeptionelle Welt" dar (Goodenough, 1971).
- **emotional:** Neben der kognitiven, analytischen Seite von Unternehmenskulturen sollte nicht die emotionale Seite vergessen werden. Denn eine Unternehmenskultur spiegelt sich ganzheitlich wider.
- **historisch:** Ein Lernprozess mit dem Umgang der externen und internen Umwelt bringt eine Unternehmenskultur hervor. Dabei geht es um teilweise tradierte Lösungswege, die sich in der Vergangenheit bewährt haben und die mithilfe der Kultur weitergegeben werden sollen (Schein, 1984).
- **interaktiv:** Eine Unternehmenskultur muss auch neuen Mitarbeitern im Unternehmen vermittelt werden. Dies geschieht durch Praktiken, die größtenteils über Symbole ausgedrückt werden. Man spricht dabei von einem Sozialisationsprozess, den beispielsweise neue Organisationsmitglieder durchlaufen müssen.

3.1.3 Kulturebenen

Edgar Schein entwickelte das in Abb. 3.2 gezeigte Kulturebenenmodell (entnommen aus [Sch99, S. 439–446]), das nicht nur beschreiben soll, wie sich die kulturelle Kernsubstanz durch einen Interpretationsprozess erschließt, sondern auch die Beziehungen der Ebenen untereinander darstellt. Vorteil dieses Modells besteht in

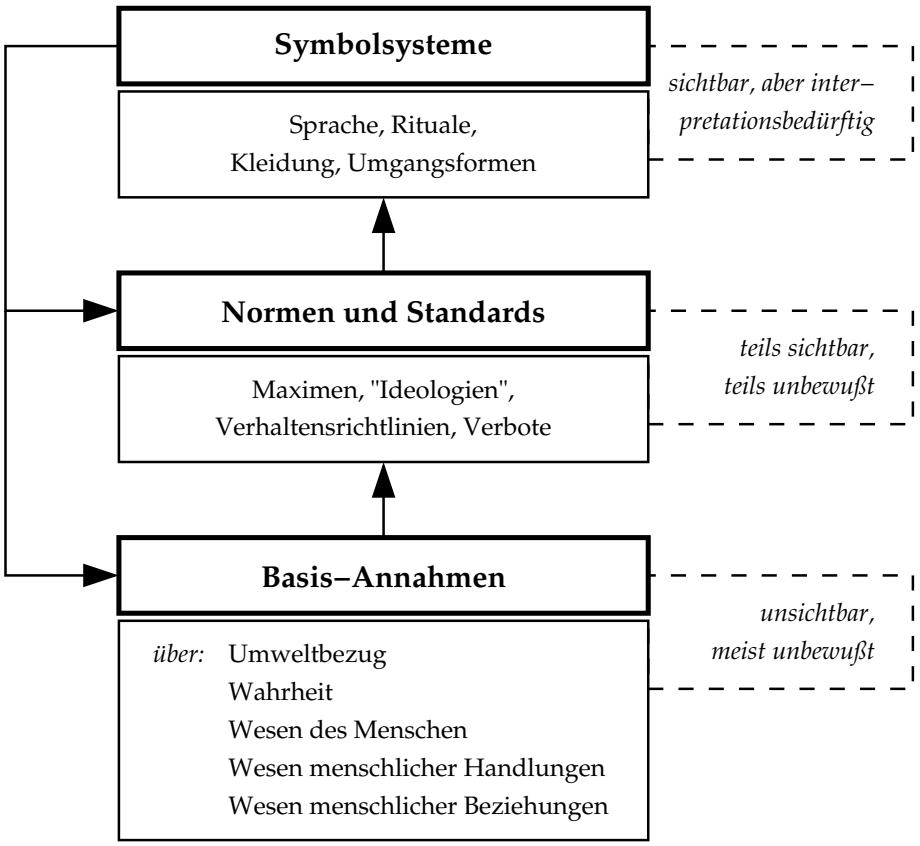

Abbildung 3.2: Kulturebenen und ihr Zusammenhang nach Schein (1984)
(Quelle: Georg Schreyögg [Sch99])

der Möglichkeit des sukzessiven Rekonstruierens und Verstehens von Unternehmenskulturen.

Die *unterste Ebene*, die Basis-Annahmen, steht für die meist unbewussten, fundamentalen Muster – beispielsweise zur Orientierung, wie der Weltanschauung –, die die Wahrnehmung sowie das Handeln beeinflussen. Sie setzt sich zusammen aus „Grundthemen menschlicher Existenzbewältigung“, also Annahmen über die Umwelt, zwischenmenschliche Beziehungen, die Natur des Menschen und seine Handlungen sowie Vorstellungen von Wahrheit (Kluckhohn/Strodtbeck, 1961, und Kirsch/Trux, 1981).

Die Basis-Annahmen zusammengenommen bilden eine Gesamtgestalt, auch „Weltbild“ genannt, dessen Werte sich in Verhaltensstandards, Verboten und Maximen widerspiegeln. Es gibt Unternehmensleitungen, die in dieser *zweiten Ebene* aus den Orientierungsmustern eine Management-Philosophie entwerfen.

Um diese Werte auch an neue Mitglieder weitergeben bzw. sie einfach leben und weiterentwickeln zu können, entstehen Symbolsysteme (*dritte Ebene*), die sich durch sichtbare Merkmale, wie Rituale (Feiern, Betriebsausflüge etc.), Kleidung oder Umgangsformen, auszeichnen. Es wird ebenfalls die Gestaltung der Räume und Gebäude als auch Initiations- und Entlassungsriten darunter verstanden.

3.2 Klassifikation von Unternehmenskulturen

3.2.1 Unternehmenskultur-Typen

Da eine Kulturgestalt nicht systematisch erfasst werden kann, wurde versucht, sie zu typisieren. Die gebräuchlichste Typisierung stammt von Terrence Deal/A. Kennedy (1982), die ich in Tab. 3.1 beispielhaft visualisiert habe (aus [Sch92, S. 1529]). Die beiden auf den Achsen abgetragenen Faktoren, die Deal/Kennedy gewählt haben, sind das Feedback und das Risiko, das einer Unternehmung zugrunde liegt.

Ebenfalls sehr verbreitet ist die Typologie von Kets de Vries/Miller (1986) (aus [Sch99, S. 446–449]), die hinsichtlich Scheins Kulturebenenmodell aus Abb. 3.2 versucht, näher an die Rekonstruktion sowie Interpretation der Basis-Annahmen zu kommen.

Da aber in der Realität eine Unternehmenskultur multifaktoriell geprägt ist, kann eine Typologie nur eine selektive Reduktion darstellen und somit nicht die Gesamtheit ausdrücken. Je nach Modell hat das seine Vor- und Nachteile.

rasch *Feedback* langsam	Brot und Spiele-Kultur („work hard / play hard“)	Alles oder nichts-Kultur („Tough-guy, macho“)
	Prozess-Kultur	Analytische Projektkultur („Bet your company“)
	gering — *Risiko* — hoch	

Tabelle 3.1: Unternehmenskultur-Typen nach Deal/Kennedy (1982)
(Quelle: Georg Schreyögg [Sch92])

3.2.2 Klassifikation nach Paul Bate

Eine aktuellere Klassifikation von Unternehmenskulturen beschreibt Paul Bate in seinem Buch „Cultural Change – Strategien zur Änderung der Unternehmenskultur“ [Bat97], das vier grobe Typen definiert, die hier ausführlicher erläutert werden. Ausserdem zeigt Bate dort die Möglichkeiten sowie die jeweiligen typimmanenten Schwierigkeiten auf, die einem Paradigmenwechsel einer Unternehmenskultur, also einem Kulturwandel, innewohnen.

Die Aggressive Methode

Basierend auf einem heroischen Kulturbewußtsein versuchen die Anhänger der Aggressiven Methode[i] die Welt, in diesem Falle das Unternehmen, zu ordnen. Das Unternehmen gilt es zu beherrschen und das omniexistente Chaos prometheisch zu besiegen (Sorokin, 1966). Vorherrschend ist eine harte Männerkultur, die sich der „unterschwelligen militärischen Metaphorik“ (Garsombke, 1988) bedient, wie ein Unternehmen „mit dem Maschinengewehr [zu] führen“ (Brissy, 1989), und versucht, durch „Unterdrückung von Alternativsichtweisen den Wandel durchzudrücken“. Sie fordert blindes Vertrauen und Gehorsam von den Untergebenen und betreibt Kulturvandalismus bezogen auf die Unternehmenskultur, indem sie sie nachhaltig schädigt. Dieser autoritäre, militärisch geprägte Führungsstil differenziert nicht nach dem Arbeiter- bzw. Angestelltentyp.

Die häufigsten Werkzeuge bei derartigen Kulturdirektiven sind Entlassung, Degradierung und Mobbing. „Wenn ich die Leute halb im Unklaren lasse, ob sie

i englisch: aggressive approach

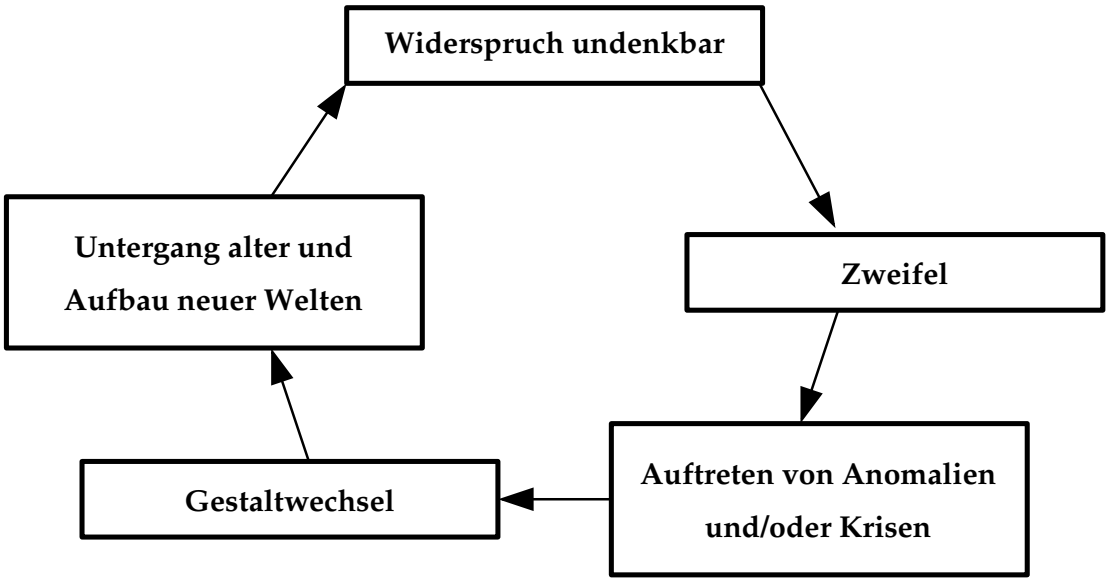

Abbildung 3.3: Paradigma-Wechsel
(Quelle: Otto-Peter Obermeier [Obe99b])

morgen Arbeit haben, werden sie wahrscheinlich viel eher machen, was ich will.“, ist die Überzeugung vieler Manager [Bat97]. Diese Taktiken finden häufig dann Anwendung, wenn das Management die ersten problematischen Anzeichen vor sich hergeschoben hat bzw. sich niemand einer Krise bewußt werden, geschweige denn sich ihrer annehmen wollte, also zu dem Zeitpunkt, an dem es für eine starre, konservative Unternehmenskultur zu spät ist, sich der neuen Herausforderung innovativ und dynamisch anzupassen.

Sie muß sich auf ein wesentlich gefährlicheres Abenteuer einlassen, als dies bei einer kontinuierlichen Veränderung der Fall gewesen wäre; nämlich die totale Verwerfung von alten Paradigmen, um eine besser funktionierende Unternehmenskultur hervorzubringen.

Dieser in Abb. 3.3 dargestellte Paradigmen-Wechsel beginnt an der Stelle, an das bestehende Modell hinterfragt wird und Zweifel auftauchen, weil sich das alte Erklärungsmuster in Widersprüche verwickelt oder sich Krisen abzeichnen. Also wird auf die Suche nach einem neuen Erklärungsmodell (Gestaltwechsel, Aufbau neuer Welten) gegangen. Die neuen Paradigmen scheinen am Anfang selbst wieder widerspruchslos zu gelten, bis auch sie hinterfragt werden und Anomalien aufzeigen.

Diese autoritäre Verwerfung, auch als „Big-Bang-Methode“ bezeichnet, die von einem behavioristischen Menschenbild ausgeht, zerstört die alte Kultur restlos; es wird hier auch von „kultureller Brandstiftung“ gesprochen [Bat97].

Nach einer derartigen kulturellen Brandstiftung entsteht in der Belegschaft ein Verlangen nach neuen Strukturen. Doch entgegen der autoritär verordneten Homogenisierung geht eine nicht gewollte pluralistischere Kultur hervor, da die Mitarbeiter in „wildem Segmentalismus“ und mit „gespaltener Loyalität“ [Bat97] sich eine neue Ordnung schaffen wollen. Eine derartige neue Ordnung scheint entgegen der geforderten hierarchischen zu arbeiten und die Autorität zu untergraben. Um aber trotzdem zu ihrer Kulturhegemonie zu kommen, wird sich die herrschende Gruppe informeller Rückmeldeverfahren bedienen, um über ein Spion- und Informantennetz eine Gedankenkontrolle ausüben und geeignete Maßnahmen gegen eine subversive Gegenkultur anwenden zu können [Bat97].

Trotz dieser negativen Auswirkungen ist die „Aggressive Methode“ sehr verbreitet und scheint immer mehr Zuspruch zu finden. Vielleicht gerade dadurch bedingt, dass immer größere Existenzängste sowohl bei den Unternehmungen qua internationalem Konkurrenzdruck als auch beim Einzelnen in Form von sozialer Absicherung und Arbeitsplatzverlust entstehen, agieren die meisten Führungskräfte nach diesem militärischen Stil [Bat97].

Die partizipatorische Methode

Eine demokratieorientiertere Struktur besitzt die partizipatorische Methode[ii]: Ihr Substrat ist eine pluralistische Betrachtungsweise, die sich in einem „selbstregulierenden Gebilde natürlichen Rechts“ (Holthoon, 1987) manifestiert; grundlegend ist die Theorie des konfliktfreien Wandels ohne den „Big Bang“ (Aggressiver Weg). Aus dieser Konfliktfreiheit resultiert keineswegs eine Kultur ohne Konflikte, vielmehr sind die möglichen Interessenskonflikte von Konvergenz- anstelle von Divergenzverfahren geprägt, die keiner dialektischen Konfrontation als Prämisse bedürfen. Es herrscht gegenseitiges Vertrauen, Probleme meistern zu können.

Nicht das Management ist der Katalysator für den Paradigmenwechsel – sie müssen den Wandel nur tolerieren, genauer gesagt: sie dürfen ihn nicht behindern –, sondern alle Kulturteilnehmer partizipieren am graduellen, dynamischen Wandel; dadurch wird allen eine erkenntnistheoretische Gewissheit wie auch ein Sicherheitsgefühl bei der Kulturmetamorphose vermittelt. Die Unternehmensleitung nimmt sich hier nicht heraus, allwissend sowie omnipotent zu sein und all ihre Macht und Energie zur Kontrolle und Überwachung zu gebrauchen. Ferner

ii englisch: conciliative approach

vertraut auch sie auf den pluralistischen Diskurs, der sich durch Flexibilität, Entgegenkommen und Egalität auszeichnet. „Er ist ein Potpourri oder Gemisch aus allen möglichen Themen, Stilen und Zielen“ (Sorokin, 1966).

Interessant erscheint, dass die anfänglichen kulturellen Veränderungen von den Betroffenen nicht wahrgenommen werden, obwohl sie sie ja selbst initiiert haben. Später erst bemerken sie ihr eingeleitetes Änderungsprogramm.

Nach [Bat97] bilden beobachteter Machtmangel, Konfliktverhütung, Kontinuität, gleichzeitige Konstruktion und Dekonstruktion der Kultur sowie Kompetenz und Veralterung die Grundprinzipien des partizipatorischen Weges.

Der Weg über informale Netze

Paul Bate [Bat97] sieht den Kulturwandel bei informalen Netzen[iii] als einen politischen Prozeß, der sich die Umverteilung der Macht und der Autorität zum Ziel nimmt. Umverteilung deswegen, weil die Anhänger dieser Methode davon ausgehen, dass eine informale Gruppe nur dann ihre Ideen durchsetzen kann, wenn sie sich gleichzeitig auf Kosten anderer Macht aneignet; ein sogenanntes „Nullsummenspiel“, was bedeutet, dass die informale Macht in einem Betrieb – wie bei einem gesättigten Markt das Marktvolumen – begrenzt ist. Der Wandel geschiet zwar gemeinsam und bewusst – ähnlich der partizipatorischen Methode –, aber bei einem politischen Netzwerk kann niemand seinem Nächsten trauen (Douglas, 1987). Jeder ist jedem ein potentieller Feind (Sorokin, 1966). Es gibt weder gemeinsam entwickelte Lösungsansätze noch Offenheit bzw. Entgegenkommen, sondern man versucht, seine Handlungen und Entscheidungswege geheim zu halten. Ein typisch politischer Diskurs (Conolly, 1974) prägt den Kulturwandel.

Doch trotz der Rangeleien um informale Macht gelingt es keiner Gruppierung, ihre ganzen Ansichten der „Opposition“ aufzuzwingen und die Macht an sich zu reißen, es besteht also quasi ein Gleichgewicht an betrieblichen Interessensgegensätzen. Vielmehr versuchen die Einzelnen, die Beziehungen anderer geschickt für sich zu manipulieren oder – wie bei einer Börse – Gefälligkeiten zu kaufen und zu verkaufen. Die Besitzer mit den meisten und präzisesten Informationen haben dadurch einen Vorsprung. Dabei dient die offizielle, formale Struktur des Unternehmens dazu, die informalen Entscheidungen umzusetzen und nach außen ein einheitliches Bild zu erzeugen.

Diese partizipatorischen, gemeinschaftlichen Prozesse sind essentiell für einen

iii englisch: corrosive approach

Kulturwandel sowie dessen Entwicklung [Bat97]. Partizipatoren eines Systems informaler Wege sind alle, denn durch jeglichen menschlichen Kontakt und ihre Interaktion entstehen informale Netzwerke, die Barnard (Barnard, 1938) als eine natürliche Folge bezeichnet. Ihre wesentlichen Elemente sind Aktion und Interaktion sowie Spannung, u.a. bedingt durch „Informationsschieberei“.

Umerziehung als Weg

Im militärischen Milieu ist neben der „Aggressiven Methode“ die Methode der Umerziehung[iv] zu finden. Ihr liegt ein kognitiver Imperialismus, ein vom „Schüler“ bewusst wahrgenommenes Oktroyieren der (neuen) Unternehmenskultur, zugrunde, die auf eine einheitliche, nicht-pluralistische, rituell geprägte Kultur – auch beschrieben als „Modellmonopol“ (Bråten, 1973) – abzielt.

Auf dieses von der Unternehmensleitung geforderte Modell müssen alle eingeschworen werden; aber das allein reicht nicht. Den Kulturteilnehmern wird verständlich gemacht, dass eine Umerziehung das beste für ihr Unternehmen ist. Deshalb kommt eine positive Einsicht der Teilnehmer über den Sinn und Zweck schnell zustande. Umgesetzt werden diese Ausbildungsprogramme durch verschiedene Arten von Riten. Die wesentlichen sind die Übergangs-, die Festigungs- und die Integrationsriten, die auf Managementseminaren u.a. durch Slogans untermauert werden: „Verantwortliches Handeln besteht im Erfüllen der Vorgaben.“

Lernen heisst in diesem Kontext: Alles Alte vergessen und die vorgestellten bzw. geforderten Veränderungen ohne tiefergehendes Hinterfragen anzunehmen. Diese Fortbildung dient also nicht zur problemorientierten Wahrheits- und Lösungsfindung in den vermeintlich krisenanfälligen Bereichen. Die Umerziehung als Weg beinhaltet lediglich eine Lehrtheorie, nicht aber eine Lerntheorie. Das ist ihre Hauptschwäche. Sie ist auch nicht auf die verschiedenen Meinungen respektive speziellen Erfahrungen der „Schüler“ ausgerichtet, d.h. vom pädagogischen Standpunkt gesehen kontraproduktiv.

Die Universität von Disneyland ↪**52** verkörpert diese Art der Umerziehung, bei der ihre Unternehmenskultur, die sie „Disney Corporate Culture“ nennt, gelehrt und gefestigt werden soll. Einige Teile sind die formlose Anrede, also kein Mister und Missis, das freundliche Lächeln, der Gebrauch ausschließlich von höflichen Ausdrücken sowie eines vorgeschriebenen Wortschatzes; letzteres bedeutet, dass Wörter wie „Veranstaltung“ oder „Unfälle“ durch „Attraktion“ und „Vorfäl-

iv englisch: indoctrinative approach

Wort	*Substitution*
Veranstaltung	Attraktion
Unfall	Vorfall
Kunden	Gäste
Vergnügungszentrum	Park
Ordnungskräfte	Sicherheitsführer
Uniform	Kostüme

Tabelle 3.2: Sprachmaninulation der Disney Corporate Culture
(Quelle: Paul Bate [Bat97, S. 234–235])

le“ substituiert werden müssen (siehe Tab. 3.2). Es wird eine streng kontrollierte Umwelt, die durch Sprach- und Symbolmanipulationen geprägt ist, geschaffen.

Im Endeffekt hat aber sowohl für die lohn- sowie arbeitsplatzabhängigen Arbeitnehmer als auch für die „Lehrer“ eine Fehlumerziehung oder falsch durchgeführte Umschulung katastrophale Folgen. Nicht gehörte, durchaus innovative Strömungen im Betrieb werden durch diese Methode zubetoniert. Aber sie fließen informal weiter und können jede gutgemeinte Kulturveränderung unterhöhlen und zerstören, indem sie sich eine eigene Subkultur bzw. Gegenkultur schaffen.

3.2.3 Starke Unternehmenskulturen

Nach der Typologie bzw. Klassifikation von Unternehmenskulturen stellt sich die Frage, inwiefern die einzelnen Typen positiv oder negativ auf eine Unternehmung einwirken. Hier hat sich die Begrifflichkeit der „starken“ bzw. „schwachen“ Kultur gebildet, die ihre Wurzeln in der Commitment-Forschung hat und sich dadurch auszeichnet, die Verbundenheit eines Mitarbeiters zu seinem Unternehmen zu messen, oder besser, den Grad der Identifikation mit seiner Organisation auszudrücken [Sch99].

Für die Definition einer starken Unternehmenskultur werden – bedingt durch die Auffassungen und Interpretationen von „stark“ – je nach Literatur verschiedene Dimensionen gebraucht; am verbreitesten sind diese drei Kriterien:

- **Prägnanz:** Die Orientierungsmuster, Wert- und Symbolsysteme sowie Standards einer starken Unternehmenskultur sind deutlich und umfassend ausgebildet. Für die Bestimmung der Stärke gilt hier, dass der Kulturinhalt keiner

bestimmten Moral oder Ethik unterworfen ist. Einzig und allein zählt die Erfolgsträchtigkeit, d.h. ihr Inhalt kann trivial, moralisch oder unmoralisch sein.

- **Verbreitungsgrad:** Der Verbreitunggrad soll die Homogenität der Werte und Normen einer Kultur unter den Kulturteilnehmenden ausdrücken, d.h. eine starke Kultur bedeutet eine von fast allen Mitarbeitern gelebte Unternehmenskultur.
- **Verankerungstiefe:** Die unter Verbreitungsgrad beschriebene Kulturkonformität der Organisationsmitglieder kann aber zwei verschiedene Ursachen haben: Zum einen die bloße Anpassung an die Standards, um den Weg des geringsten Widerstandes zu gehen; zum anderen die *Internalisierung* des Wertesystems, also das Leben der Unternehmenskultur aus der eigenen Überzeugung heraus. Mithilfe der Verankerungstiefe soll die Verinnerlichung dieser Werte gemessen werden, die bei starken Kulturen ausgeprägter ist. Neben der Verankerungstiefe kommt der *Persistenz*, die die zeitliche Stabilität einer Unternehmenskultur beschreibt, ebenfalls Bedeutung zu.

3.2.4 Funktionale und dysfunktionale Effekte

Ein Zusammenhang zwischen Leistungsniveau und Stärke ließ sich nicht eindeutig bzw. es ließ sich nur eine schwache Korrelation nachweisen. Neuere Untersuchen ergaben, dass starke Unternehmenskulturen nicht ausschließlich positive Wirkungen haben. Es wird hier von funktionalen (positiven) und dysfunktionalen (negativen) Effekten gesprochen [Sch99].

Funktional wäre bei starken Kulturen die Handlungsorientierung, die reibungslose Kommunikation, rasche Entscheidungsfindung, zügige Implementation, geringer formaler Kontrollaufwand, Stabilität sowie Motivation und Teamgeist. *Dysfunktionale* Effekte können die Tendenz zur (inneren) Abschließung (beispielsweise, wenn ein Kulturwandel unabdingbar wäre, um das Unternehmen an eine neue Umwelt anzupassen), Abwertung neuer Orientierungen, Wandelbarrieren, Fixierung auf traditionelle Erfolgsmuster oder „Kulturdenken“ (Kulturkonformität wird erzwungen) sein. [Sch99]

3.3 Unternehmenssicherheit und -kultur

Eine starke Unternehmenskultur – wie sie in der Studie von Pricewaterhouse-Coopers [MS01] propagiert wird – scheint per Definition auch starke negative (dysfunktionale) Effekte zu haben. So muss die Frage gestellt werden, welcher Mitarbeiter sich in welcher Unternehmenskultur risikobewusst verhalten kann. Was für Unternehmenskulturen nach der Bate-Klassifikation [Bat97] (3.2.2) vorzuziehen ist, scheint eindeutig zu sein. Je nach Sparte eines Unternehmens gibt es sicherlich verschiedene Meinungen, welche Kultur zu einem Unternehmenstyp am besten passt bzw. aus was für einem Unternehmenstyp eine bestimmte Kultur hervorgeht; jedoch sollte in risikobelasteten und innovationsorientierten Bereichen versucht werden, eine demokratische und kooperative, d.h. eine informale oder partizipatorische, und keine autokratische – wie bei der Agressiven Methode oder der Umerziehung – Unternehmenskultur zu fördern und zu leben.

Den idealen Führungsstil gibt es zwar nicht, aber er ist auf jeden Fall kooperativ geprägt, das ist „heute keine Forderung mehr, sondern eine Selbstverständlichkeit“ [NS88, S. 211]. Der Leitende übernimmt wichtige Kohäsions- und Lokomotionsfunktionen [NS88], das bedeutet auch, dass Mitarbeiter an der Entwicklung von Sicherheitsanwendungen partizipieren sollten und dazu ermuntert werden müssen.

In einer risikoorientierten Unternehmenskultur können einige Maßnahmen unterstützend wirken: So ist die Rede von der Einführung von **„Quality Circles“**, bei denen auf freiwilliger Basis sich Mitarbeiter einer Abteilung zusammenfinden, um selbst ausgewählte Probleme und Schwachstellen aus dem eigenen Arbeitsbereich zu analysieren. Problemlösungen, Ideen, Verbesserungsvorschläge können von ihnen eingebracht werden. Sie stellen eine Form des **„Betrieblichen Vorschlagswesens“** (BVW) dar, dass auf jeden Fall eingeführt oder reaktiviert werden sollte. [NS88]

3.3.1 Kommunikation

Eine nachhaltige Identifikation eines Kulturteilnehmers mit seinem Unternehmen kann am besten dann stattfinden, wenn auch seine Wünsche und Emotionen gehört und berücksichtigt werden, d.h., dass alle Dimensionen der Kommunikation – von kognitiv, emotiv bis zu habituell – angesprochen werden [Obe99b].

Laut einer Untersuchung (Neuberger, 1973) beansprucht der Vorgesetzte ungefähr 80% der Redezeit in Mitarbeitergesprächen [NS88]. Das zeigt, dass die Kommunikationspartner nicht gleichberechtigt diskutieren können, woraus ein Vermeiden von risikoorientierter Kommunikation resultieren kann. Die „Risikokommunikation“ – nach der Risikogesellschaft einer neuer Begriff in diesem Zusammenhang – beschäftigt sich mit der Untersuchung von risiko- und lösungsorientierter Kommunikation. [GO94, GO95, Obe99a].

Links

52 http://www.disney.com/

4 Ausblick

Diese Arbeit hat mir gezeigt, wie komplex die Gebiete rund um die Unternehmenssicherheit sind. Die Schwierigkeit einer interdiziplinären Arbeit liegt in der richtigen Zusammenstellung der Themengebiete. Diesem gerecht zu werden erscheint fast unmöglich, da es keine Abgrenzung gibt, die jedem Sachverhalt zu seinem Stellenwert verhilft. Ich denke, mit meiner Einteilung ein ausgewogenes Verhältnis geschaffen zu haben.

Die juristische Seite im ersten Kapitel hatte ich mit den aktuellen Gesetzesvorhaben, wie die europäischen ENFOPOL-Pläne oder dem US-amerikanischen „Patriot-Act“, füllen wollen, aber ich beschränkte mich auf die für Deutschland zur Zeit geltende und zukünftige Rechtslage (ENFOPOL könnte auch dazugezählt werden).

Das zweite Kapitel hätte ich gern ausführlicher behandelt, doch allein der Bereich der IT-Sicherheit könnte Bücher füllen. Von „Public Key Infrastructure“ und „Zertifizierungsauthoritäten“ (CA) bis hin zu einer detaillierteren Beschreibung von Cracker-Angriffen und der Benutzbarkeit von Sicherheitsanwendungen fallen mir viele Inhalte ein, die ebenfalls interessant gewesen wären.

Ich hätte mir gewünscht, noch das Buch „Competetitive Intelligence“ von Lux und Peske ↪**53** einbeziehen zu können, das im Juli 2002 erscheinen sollte, aber bis dato noch nicht erhältlich ist. Zusammen mit Untersuchungen zur Wirtschafts- und Industriespionage, Fällen – wie vom Windkrafthersteller Enercon oder dem ICE-Verkauf von Thyssen an Südkorea – und einer historischen Aufbereitung (Stichwort „Kommerzielle Koordinierung“ der DDR / „Schalck-Golodkowski“) dieser Thematik hätte ich ein interessantes Kapitel füllen können. Leider ist der Themenbereich schwer zu recherchieren und ich musste ihn deshalb vorerst aufgeben.

Links

53 http://d-nb.info/965587754

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[ats02] ATSEC: *@sec – the information security provider*. 2002. Informationsbroschüre von @sec.

[Bat97] BATE, PAUL: *Cultural Change – Strategien zur Änderung der Unternehmenskultur*. Gerling Akademie Verlag, 1997.

[Bra02] BRAUCH, PATRICK: *Sicherheits-Studie: Hybrid-Angriffe im Kommen*. Heise newsticker, April 2002. http://heise.de/-59552.

[BSI02a] BSI: *Deutsche IT-Sicherheitszertifikate – Sicherheit von IT-Produkten und -Systemen*. Bundesamt für Sicherheit in der Informationstechnik, März 2002.

[BSI02b] BSI: *IT-Sicherheitszertifizierung*. BSI-Informationen zu Fachthemen, 2002. http://www.bsi.bund.de/literat/doc/ancczer.htm.

[Bun01a] BUNDESGESETZBLATT: *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften*. Bundesgesetzblatt Teil I Nr. 22 vom 21.05.2001, Seiten 876–884, Mai 2001.

[Bun01b] BUNDESKRIMINALAMT: *Polizeiliche Kriminalstatistik 2000*. 2001. http://www.bka.de/pks/pks2000/.

[BY02] BELCHER, TIM und ELAD YORAN: *Riptech Internet Security Threat Report – Attack Trends for Q3 and Q4 2001*. Riptech Inc., Jan. 2002.

[CMM+02] CONRAD, MICHAEL, ULRICH MOHR, STEFAN MINK, FRANK PÄHLKE und MARCUS SCHÖLLER: *Eine modulare Netfilter-basierte IPSec-Implementierung*. LinuxTag 2002, Juni 2002.

[Cox01] COX, JOHN: *Serious security weakness in 802.11b wireless LANs exposed*. Network World Fusion, Aug. 2001. http://www.nwfusion.com/news/2001/0806ieee.html.

[Cri02] CRIADO, MIGUEL ÁNGEL: *De Moncloa al 'Marca', diario de un 'Hacker'*. El Mundo – ARIADN@, Cibersociedad, (90.):2, Abril 2002.

[Egg96] EGGER, EDELTRAUD: *Datensicherheit und Datenschutz – Technische und rechtliche Perspektiven*, Kapitel 12. Grundlagen der Datensicherheit, Seiten 211–216. StudienVerlag, 1996.

[FMS01] FLUHRER, SCOTT, ITSIK MANTIN und ADI SHAMIR: *Weakness in the Key Scheduling Algorithm of RC4*. 2001. http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf.

[Fox00] FOX, DIRK: *Data Encrytion Standard (DES)*. Datenschutz und Datensicherheit, (24):736, Dez. 2000.

[Fox02] FOX, DIRK: *Computer Emergency Response Team (CERT)*. Datenschutz und Datensicherheit, (26):493, Aug. 2002.

[Fug96] FUGINI, MARIA GRAZIA: *Datensicherheit und Datenschutz – Technische und rechtliche Perspektiven*, Kapitel 16. Datensicherheitsmaßnahmen in Betriebssystemen und Datenbanken, Seiten 311–337. StudienVerlag, 1996.

[Gas02] GAST, MATTHEW: *Wireless LAN Security: A short History*. O'Reilly Network, April 2002. http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html.

[Gib02] GIBSON, STEVE: *The Strange Tale of the Denial of Service Attacks against GRC.COM*. März 2002. http://grc.com/dos/grcdos.pdf.

[GO94] GERLING, ROLF und OTTO-PETER OBERMEIER: *Risiko – Störfall – Kommunikation*. Gerling Akademie Verlag, 1994.

[GO95] GERLING, ROLF und OTTO-PETER OBERMEIER: *Risiko – Störfall – Kommunikation 2*. Gerling Akademie Verlag, 1995.

[Hof01] HOFSTEDE, GEERT: *Lokales Denken, globales Handeln*. Beck–Wirtschaftsberater im dtv, 2. Auflage, 2001.

[Iac02] IACONO, LUIGI LO: *Rote Telefone – Abhören von IP-Telefonaten*. iX – Magazin für professionelle Informationstechnik, (No. 5):118–119, Mai 2002.

[Jae98] JAEGER, STEFAN: *Computerkriminalität*. Interest Verlag, 1998.

[Kin01] KING, JASON S.: *An IEEE 802.11 Wireless LAN Security White Paper*. Okt. 2001. http://www.llnl.gov/asci/discom/ucrl-id-147478.html.

[Kop00] KOPKA, HELMUT: *LaTeX– Band 1: Einführung*. Addision–Wesley, 3. Auflage, 2000.

[Kre00] KREMPL, STEFAN: *17C3: Wau Holland bläst zur Meinungsfreiheits-Offensive*. Heise newsticker, Dez. 2000. http://heise.de/-27208.

[Kuh02] KUHN, MARKUS G.: *Optical Time-Domain Eavesdropping Risks of CRT Displays*. Proceedings 2002 IEEE Symposium on Security and Privacy, Mai 2002. http://www.cl.cam.ac.uk/ mgk25/ieee02-optical.pdf.

[Lem02] LEMOS, ROBERT: *Study: Hackers take a trip through Asia*. ZDNet News, März 2002. http://zdnet.com.com/2100-1105-862936.html.

[LW00] LUCKS, STEFAN und RÜDIGER WEIS: *Der DES-Nachfolger Rijndael*. Datenschutz und Datensicherheit, (24):711–713, Dez. 2000.

[Mac02] MACKENBROCK, MARKUS: *Common Criteria und Schutzprofile – Standard für die Prüfung und Bewertung der Sicherheit von Informationstechnik*. In: *Vortragveranstaltungen zu den aktuellen Themen der IT-Sicherheit*. Bundesamt für Sicherheit in der Informationstechnik, März 2002.

[Med01] MEDOSCH, ARMIN: *Netzpiraten – Die Kultur des elektronischen Verbrechens*, Kapitel 3. The Kids are out to play, Seiten 117–127. Verlag Heinz Heise, 2001.

[MS01] MAUL, KARL-HEINZ und STEFFEN SALVENMOSER: *Europäische Umfrage zur Wirtschaftskriminalität 2001 – Industriestudie Pricewaterhouse-Coopers*. Fachverlag Moderne Wirtschaft, 2001.

[MVS01] MOORE, DAVID, GEOFFREY M. VOELKER und STEFAN SAVAGE: *Inferring Internet Denial-of-Service Activity*. 2001. http://www.caida.org/outreach/papers/backscatter/.

[NS88] NÜTTEN, INGEBORG und PETER SAUERMANN: *Die anonymen Kreativen – Instrumente einer innovationsorientierten Unternehmenskultur*. Verlag Gabler, 1988.

[Obe99a] OBERMEIER, OTTO-PETER: *Die Kunst der Risikokommunikation*. Gerling Akademie Verlag, 1999.

[Obe99b] OBERMEIER, OTTO-PETER: *Zur Philosophie des Unternehmertums und dem Umgang mit Unsicherheit*, Wintersemester 1998/1999. Vortrag im Humboldt-Zentrum der Universität Ulm.

[Pax01] PAXSON, VERN: *An analysis of using reflectors for distributed denial-of-service attacks*. ACM SIGCOMM – Computer Communication Review, Seiten 38–47, 2001.

[Pow02] POWER, RICHARD: *CSI/FBI Computer Crime and Security Survey 2002*. Computer Security – Issues & Trends, (Vol. VIII, No. 1), Frühling 2002. http://www.gocsi.com/pdfs/fbi/FBI2002.pdf.

[RC01] RUSSELL, RYAN und STACE CUNNINGHAM: *Das Hacker-Buch*. mitp-Verlag, 2001.

[Sch92] SCHREYÖGG, GEORG: *Handwörterbuch der Organisation*, Kapitel Organisationskultur, Seiten 1525–1537. Poeschel Verlag, 3. Auflage, 1992.

[Sch99] SCHREYÖGG, GEORG: *Organisation – Grundlagen moderner Organisationsgestaltung*. Gabler Verlag, 3. Auflage, 1999.

[Sch00] SCHNEIER, BRUCE: *Secrets & Lies – Digital Security in a Networked World*. Wiley Computer Publishing, 2000.

[Sch01] SCHMIDT, JÜRGEN: *Trügerische Sicherheit mit automatischen IP-Sperren*. Heise newsticker, Dez. 2001. http://heise.de/-51823.

[Sch02] SCHMIDT, JÜRGEN: *Rückhaltlose Veröffentlichung von Sicherheitslücken erwünscht*. Heise newsticker, Juli 2002. http://heise.de/-62069.

[SCJ00] STEVENSON, GORDON und CLIVE CARMICHAEL-JONES: *The Enemy Within – Investigating Computer Crime in the 21st Century*. Vogon International Limited, 2000.

[SH02] SCHULZKI-HADDOUTI, CHRISTIANE: *IT-Sicherheit nur ein lästiges Übel?* ct – Magazin für Computertechnik, (14):28, Juli 2002.

[Smi02] SMITH, RICHARD: *Country Threat: An Analysis of Internet Attacks*. Predictive Systems, 2002. http://www.predictive.com/pdf/Country_Threat.pdf.

[SO02] SKOUDIS, ED und CHRIS O'FERRELL: *Ethical Hacking – Are your bases covered?* Predictive Systems, 2002. http://www.predictive.com/publications/articles/article_detail.cfm?Rsc_ID=309.

[StG94] STGB: *Strafgesetzbuch*. Beck-Texte im dtv, 29. Auflage, 1994.

[Str91] STRAUSS, CHRISTINE: *Informatik-Sicherheitsmanagement – Eine Herausforderung für die Unternehmensführung*. Teubner, 1991. Dissertation Universität Zürich.

[Tox01] TOXEN, BOB: *Real World Linux Security – Intrusion Prevention, Detection and Recovery*. Prentice Hall, 2001.

[VB01] VERTON, DAN und BOB BREWIN: *Researchers break wireless LAN encryption algorithm*. Computerworld, Aug. 2001. http://www.nwfusion.com/news/2001/0810wlan.html.

[Zot00] ZOTA, VOLKER: *Schlechte Aussichten für „Mafiaboy"*. Heise newsticker, August 2000. http://heise.de/-25501.