Institut für Rundfunkökonomie
an der Universität zu Köln

Dirk Slama

Das Schwarzseher-Problem beim Pay-TV

Arbeitspapiere
des Instituts für Rundfunkökonomie
an der Universität zu Köln

Heft 203

Köln, im Juli 2005

Arbeitspapiere des Instituts für Rundfunkökonomie

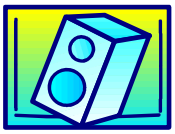
ISSN der Arbeitspapiere: 0945-8999
ISBN des vorliegenden Arbeitspapiers 203: 3-934156-97-5

Schutzgebühr 19,-- €

Die Arbeitspapiere können im Internet eingesehen
und abgerufen werden unter der Adresse
http://www.rundfunk-institut.uni-koeln.de

Mitteilungen und Bestellungen richten Sie bitte per Email an:
rundfunk-institut@uni-koeln.de
oder an die u. g. Postanschrift

Kritik und Kommentare zur vorliegenden Arbeit werden
ebenfalls an die obigen Anschriften erbeten oder direkt an die
Email-Adresse des Verfassers: slama.dirk@web.de



Institut für Rundfunkökonomie
an der Universität zu Köln

Hohenstaufenring 57a
D-50674 Köln
Telefon: (0221) 23 35 36
Telefax: (0221) 24 11 34

Dirk Slama

Das Schwarzseher-Problem beim Pay-TV*

---

* Die vorliegende Arbeit wurde im SS 2005 an der Wirtschafts- und Sozialwissenschaftlichen Fakultät der Universität zu Köln als Diplomarbeit angenommen.

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abo	Abonnement
AEPOC	Association Européenne pour la Protection des Œuvres et Services Cryptés
AFRTS	Armed Forces Radio and Television Service
AG	Aktiengesellschaft
ARPU	Average Revenue Per User
BGB	Bürgerliches Gesetzbuch
CA	Conditional Access
CAM	Conditional Access Modul
CAS	Conditional Access-System
Casbaa	Cable and Satellite Broadcasting Association of Asia
CAS-ID	Conditional Access System - Identifier Data
CAT	Conditional Access Tabelle
CI	Common Interface
CSA	Common Scrambling Algorithm
CW	Control Words
DPSC	Digitale Piraten-Smartcard
DVB	Digital Video Broadcasting
DVB-T	Digital Video Broadcasting - Terrestrial
ECM	Entitlement Control Message
EMM	Entitlement Management Messages
EU	Europäische Union
KDG	Kabel Deutschland GmbH
MOSC	Modified Original Smartcard
NDS	News Digital Systems
o.J.	ohne Jahr
o.V.	ohne Verfasser
PAL	Phase Alternating Line
PCMCIA	Personal Computer Memory Card International Association
PMT	Program Map Tabelle
StGB	Strafgesetzbuch
STOP	Scandinavian TV Organisation Against Piracy
TÜV	Technischer Überwachungsverein
TV	Television
UrhG	Urheberrechtsgesetz
URL	Uniform Resource Locator
U.S.C.	United States Code
UWG	Gesetz gegen den unlauteren Wettbewerb
VERI	Verifizierte Rechte Inhaber Programm
ZKDSG	Zugangskontrolldiensteschutz-Gesetz

1. Einleitung

Das gegenwärtige Fernsehangebot bietet eine große Sender- und Programmvielfalt, die teilweise kostenpflichtig ist. Jedoch ist nicht jeder Zuschauer geneigt, Gebühren an die Pay-TV-Sender zu bezahlen und verschafft sich daher illegal Zugang zu den verschlüsselten Programmen.

Das Problem des Schwarzsehens ist so alt wie das Pay-TV selbst. 1984 startete in Frankreich der Pay-TV-Sender Canal+, nur zwei Wochen später wurden in Elektronik-Zeitschriften bereits Anleitungen zum Nachbau der Decoder veröffentlicht.[1] Pay-TV-Piraterie hat zwischenzeitlich alarmierende Ausmaße angenommen.[2] Einschätzungen von Experten zufolge wird der jährliche Umsatz auf dem Markt für Piraterie-Produkte wie Smartcards und Decodiergeräte innerhalb der Europäischen Union mit einer Milliarde Euro beziffert.[3] Im Vergleich dazu betrug im Jahr 2003 der Umsatz auf dem westeuropäischen Pay-TV-Markt 20 Milliarden Euro.[4] Zwischen 15 und 20 Prozent aller Zugangskontrollsysteme, zu denen auch die Verschlüsselungssysteme der Pay-TV-Anbieter gehören, werden schätzungsweise illegal geknackt oder manipuliert. Demnach wird angenommen, daß fast jeder dritte Konsument von Pay-TV sich seine Leistungen erschleicht und damit ein Schwarzseher ist.[5] Dies hat für die Pay-TV-Anbieter europaweit Verluste von mehreren hundert Millionen Euro pro Jahr zur Folge.[6] Der britische Anbieter ITV hat nach eigenen Angaben bis zum Jahr 2002 durch Piraterie 100 Millionen Pfund verloren.[7] Der Verlust durch entgangene Einnahmen in den USA wurde 2002 mit über einer Milliarde Dollar beziffert.[8] Daß die Fernsehpiraterie und das Schwarzsehen auch auf anderen Kontinenten ein ernst zu nehmendes Problem darstellen, zeigen die Schätzungen der Cable and Satellite Broadcasting Association of Asia (Casbaa): Sie beziffert die Verluste für die indische Pay-TV-Branche auf 565 Millionen Dollar für das Jahr 2004, für den gesamten asiatisch-pazifischen Raum ohne Australien, China und Japan wird ein Betrag von 970 Millionen Dollar genannt.[9] Für die Zukunft wird davon ausgegangen, daß die Pirateriedelikte im Bereich des Pay-TV weiter zunehmen werden.[10]

In Deutschland gewinnt die Erlösform Pay-TV zunehmend an Bedeutung. Nach dem bekanntesten deutschen Pay-TV-Anbieter Premiere starteten im Jahr 2004

---

1 Dinsel, 1991, S. 15

2 o.V., o.J.(25)

3 o.V., 2003(5) sowie o.V., o.J.(25)

4 Clover, 2004

5 Schlomski, o.J.

6 Pötzsch, 2001c

7 Röttgers, 2002

8 o.V., 2002(16)

9 Schubert, 2004b

10 o.V., 2003(3), S. 14

einige deutsche Kabelnetzbetreiber Pay-TV-Angebote. Allein die Kabel Deutschland GmbH (KDG) verzeichnete im Februar 2005 bereits ca. 100.000 Pay-TV-Kunden. Guillaume de Posch, Chef des ProSiebenSat.1-Konzerns,[11] erwartet eine Steigerung dieser Zahl in nächster Zeit auf ein bis zwei Millionen.[12] Premiere verfügt gegenwärtig über einen Kundenstamm von 3,4 Millionen Abonnenten[13] und strebt mittelfristig die vier Millionen-Grenze an.[14] Im Rahmen dieser Entwicklung gewinnt auch das Problem der Schwarzseher an Relevanz.[15]

Die vorliegende Arbeit untersucht das Schwarzseher-Problem im Bereich des Pay-TV aus zwei Perspektiven: zunächst aus der Perspektive der Pay-TV-Anbieter, anschließend aus Sicht der Pay-TV-Piraten. Hierbei ist es unerläßlich, neben den Schwarzsehern auch die Pay-TV-Hacker und die Dealer unerlaubter Pay-TV-Technik in die Betrachtung mit einzubeziehen.

Die betriebswirtschaftliche Untersuchung des Problems erfolgt schwerpunktmäßig als Kosten-Nutzen-Analyse. Im folgenden Kapitel werden zunächst die theoretischen Grundlagen für das Verständnis der Arbeit dargestellt und erläutert. Im dritten Kapitel wird ausführlich das Schwarzseher-Problem aus Sicht der Pay-TV-Anbieter diskutiert. Nach der Abgrenzung des Begriffs Pay-TV-Piraterie werden die ökonomischen Auswirkungen aufgezeigt. Anschließend werden Kosten und Nutzen der durch die Pay-TV-Anbieter getroffenen Bekämpfungsmaßnahmen analysiert. Diese umfassen die indirekte Bekämpfung durch den Ausschluß der Schwarzseher mit technischen Mitteln sowie die direkte Bekämpfung der Pay-TV-Piraten. Dabei wird auch auf die juristischen Grundlagen eingegangen.

Im sich anschließenden vierten Kapitel erfolgt die Analyse aus Sicht der Pay-TV-Piraten. Zunächst werden hier die Kosten für einen legalen Pay-TV-Zugang ermittelt. Diesen werden daraufhin die Kosten für einen illegalen Zugang gegenübergestellt. Dabei werden nicht nur die direkten Kosten für Entwicklung und Kauf von Schwarzseher-Equipment betrachtet, auch die Risiken, die Pay-TV-Piraten eingehen, und psychologische, nicht-monetäre Momente finden Berücksichtigung.

---

[11] Die ProSiebenSat.1 Media AG plant selbst einen eigenen Pay-TV-Kanal in Deutschland, der ab Herbst 2005 im Kabelnetz von Kabel Deutschland auf Sendung gehen soll (Busse, 2005). In den USA wird seit Februar 2005 der deutschsprachige Sender „ProSiebenSat.1 Welt“ als Pay-TV-Angebot ausgestrahlt (Buschendorf, 2005a).

[12] Busse, 2005

[13] ebenda

[14] Wadlinger, 2005

[15] Allerdings scheinen gegenwärtig nicht alle Pay-TV-Anbieter sich mit der Schwarzseher-Problematik ernsthaft auseinander zu setzen. So sind für den Kabelnetzbetreiber „ish“ Schwarzseher beim digitalen Pay-TV „kein Thema“, da die verwendete Nagravision-Verschlüsselung z.Zt. sicher ist (Krüger, 2004). Jedoch hat die Vergangenheit gezeigt, daß es nur eine Frage der Zeit ist, bis sich für eine Verschlüsselung eine Umgehungslösung finden läßt.

Im fünften Kapitel erfolgt eine Zusammenführung der beiden Perspektiven, indem aus den vorher erarbeiteten Informationen Handlungsempfehlungen abgeleitet werden. Dabei wird neben erfolgversprechenden Maßnahmen im Kampf gegen die Piraterie auch auf die optimale Intensität der Schwarzseher-Ausschlussbemühungen durch Pay-TV-Anbieter eingegangen.

In Kapitel 6 erfolgt vor dem Hintergrund der Schwarzseher-Problematik eine Einordnung von Pay-TV als ökonomisches Gut.

Im Verlauf der Untersuchung erwies es sich häufig als schwierig, konkrete unternehmensinterne Daten hinsichtlich der Auswirkungen der Piraterie auf die Geschäftstätigkeit der Pay-TV-Anbieter zu erhalten. Die Ursachen für die Zurückhaltung bei der Informationsversorgung sind hinter befürchteten Auswirkungen auf das Vertrauen der Kunden in die Qualität des vorhandenen Schutzes, auf die Wettbewerbsposition im Markt und auf den Shareholder-Value zu vermuten.[16] Für die folgende Analyse können daher oft nur theoretische Betrachtungen der Kosten- und Nutzenaspekte oder beispielhafte Darstellungen erfolgen.

Die Grundlage dieser Arbeit beruht auf dem Studium vor allem von betriebs- und volkswirtschaftlichen Monographien, Sammelbänden, Zeitschriftenartikeln, Dissertationen und Arbeitspapieren. Insbesondere das Internet erwies sich während der Recherchen als wichtige Ressource. Als Quelle dienten hier nicht nur die Internetseiten von Fachmagazinen, Nachrichtendiensten, Pay-TV-Anbietern und -Organisationen, auch der Besuch von Foren und Pay-TV-Hacker-Seiten erwies sich für das Verständnis und die Verifizierung von Beschaffungsmöglichkeiten theoretisch beschriebener illegaler Pay-TV-Zugangsmethoden als hilfreich. Allerdings wurde keine der illegalen Zugangsmethoden durch den Verfasser tatsächlich getestet, so daß bzgl. der Funktionsfähigkeit der verschiedenen Zugänge den angegebenen Quellen Glauben geschenkt werden muss.

[16] o.V., 2003(3), S. 15

2. Theoretische Grundlagen

2.1. Der homo oeconomicus und die Theorie des rationalen Handelns

Jeder Mensch hat Bedürfnisse, die er befriedigen möchte. Mittel der Bedürfnisbefriedigung stellen Güter, sowohl Sachgüter als auch Dienstleistungen, dar. Die Befriedigung der Bedürfnisse durch den Konsum der Güter stiftet Nutzen. Werden Güter konsumiert, deren Vorrat sich nicht erschöpft und für deren Gewinnung keine Anstrengungen notwendig sind, für sie also keine Knappheit vorliegt, handelt es sich um freie Güter. In der Realität sind die meisten Güter jedoch knapp, d.h. es liegt eine Diskrepanz vor zwischen der Gütermenge, die tatsächlich vorhanden oder erreichbar ist, und der Menge, die zur Bedürfnisbefriedigung gewünscht ist: Die Güternachfrage übersteigt das Güterangebot. Diese nicht freien Güter werden als wirtschaftliche Güter bezeichnet. Da die Bereitstellung der wirtschaftlichen Güter Kosten verursacht, sind die Wirtschaftssubjekte gezwungen, wirtschaftlich zu handeln. Wirtschaften bedeutet, Wahlentscheidungen aufgrund bestimmter Kriterien zu treffen, da in den meisten Fällen aufgrund beschränkter Mittel nicht alle Bedürfnisse befriedigt werden können und daher zwischen verschiedenen Alternativen ausgewählt werden muss.[17] Weil das Fällen von Entscheidungen mit Zielkonflikten verbunden ist, wird bei der Entscheidungsfindung zwischen Kosten und Nutzen einer Handlung und deren Alternativen abgewogen.[18] Nutzen sind Wirkungen, die hinsichtlich eines Zieles als positiv bewertet werden, negativ bewertete Wirkungen stellen entsprechend Kosten dar. Kosten sind als entgangener Nutzen alternativer Mittelverwendung stets Opportunitätskosten, der Nutzen kann dementsprechend als Opportunitätsnutzen bezeichnet werden, also als entgangene Kosten alternativer Verwendung.[19] In vielen Fällen ist es dabei erforderlich, in Grenzbegriffen zu denken. Ein rationaler Entscheider stimmt nur dann für eine Handlung, wenn der Grenznutzen, dies ist der Nutzen einer zusätzlichen Einheit, die Grenzkosten, also die Kosten einer weiteren Einheit, übersteigt.[20]

Nach dem ersten Gossenschen Gesetz nimmt die Dringlichkeit eines Bedürfnisses mit zunehmender oder wiederholter Befriedigung ab. Der Grenznutzen wird also mit steigendem Güterkonsum stetig kleiner. In einer graphischen Darstellung nimmt die Nutzenkurve einen konkaven Verlauf.[21]

Abbildung 1 zeigt, dass mit einer zunehmender Menge x der Nutzen U(x) stetig ansteigt, jedoch mit abnehmender Zuwachsrate bzw. abnehmendem Grenznutzen.

---

[17] Woll, 1996, S. 50ff

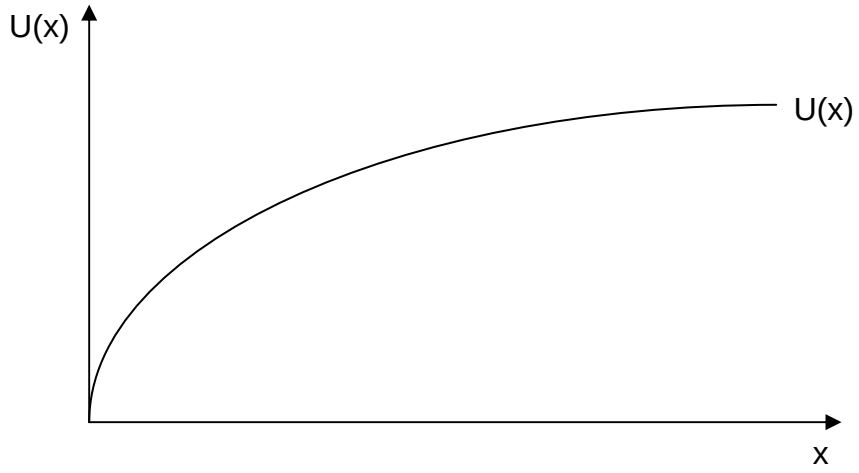
[18] Vgl. Mankiw, 2004, S. 6.

[19] Brümmerhoff, 2001, S. 196

[20] Mankiw, 2004, S. 6f

[21] Blum, 1994, S. 106

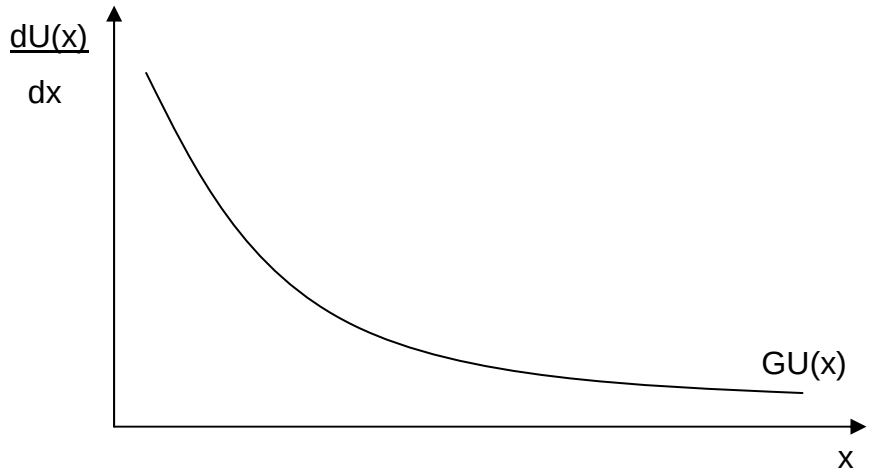
Abbildung 1:
Nutzenfunktion mit abnehmendem Grenznutzen



Quelle: Blum, 1994, S. 107

Abbildung 2 stellt den Verlauf des Grenznutzens dU(x)/dx dar. Mit zunehmender Menge x nimmt der Grenznutzen, also der Nutzen jeder weiteren Einheit, ab.

Abbildung 2:
Grenznutzenfunktion



Quelle: Blum, 1994, S. 107

Der homo oeconomicus geht bei seiner Entscheidungsfindung nach dem ökonomischen Prinzip vor. Dieses Prinzip verlangt eine Entscheidung, die zu dem bestmöglichen Verhältnis zwischen Gütereinsatz als Input und Güterentstehung als Output führt.[22] Dabei werden zwei Ausprägungen unterschieden: Entweder er berücksichtigt das Minimalprinzip, d.h. ein vorgegebenes Ziel soll mit minimalem Mitteleinsatz erreicht werden, oder er wählt das Maximalprinzip, d.h. bei

[22] Schumann, Hess, 2000.

vorgegebenem Mitteleinsatz erfolgt eine Optimierung der Ziele. Entscheidungsfindungen nach dem ökonomischen Prinzip werden als rational bezeichnet. Dies gilt für Konsumenten und Produzenten gleichermaßen.[23]

2.2. Kosten-Nutzen-Analyse

Ein Instrument, das der Entscheidungsfindung nach rationalen Kriterien dient, ist die Kosten-Nutzen-Analyse. Sie bewertet Handlungen im Hinblick auf bestimmte Ziele und liefert Informationen darüber, ob eine Handlung sinnvoll ist oder welche Alternative aufgrund des günstigsten Kosten-Nutzen-Verhältnisses ausgewählt werden sollte.[24] Sofern der Nutzen zwar gemessen, jedoch nicht (monetär) bewertet werden kann, muss nach dem Kostenminimierungsprinzip bzw. nach der Kosten-Wirksamkeitsanalyse verfahren werden. Das Kostenminimierungsprinzip entspricht dem Minimalprinzip, d.h. das festgelegte angestrebte Ergebnis soll auf die Weise erreicht werden, die die minimalen Kosten verursacht. Stehen mehrere Alternativen zur Verfügung, die das Ziel nur zu einem unterschiedlichen Grad erreichen können, wird die Kosten-Wirksamkeitsanalyse angewandt.[25]

Im betriebswirtschaftlichen Bereich kommt dem Kostenbegriff neben dem volkswirtschaftlichen Opportunitätskonzept vor allem eine monetäre Bedeutung zu, d.h. ein Unternehmer kalkuliert in seiner Kostenrechnung, wie viel er für eine Leistung zu bezahlen hat. Die betriebs- und die volkswirtschaftliche Verwendung des Kostenbegriffs kann kongruent sein, muss es aber nicht.[26]

Der in Abbildung 3 dargestellte Kostenverlauf weist zunehmende Grenzkosten auf, d.h. mit zunehmendem x steigen die Kosten überproportional. Kostenverläufe können je nach Untersuchungsgegenstand unterschiedlich sein. Auch degressive oder lineare Kostenverläufe sind denkbar.

In Abbildung 4 sind Kosten- und Nutzenverlauf in einer Graphik zusammengefasst. Die mittlere Kurve ist die Resultierende aus Kosten und Nutzen. Sofern Kosten und Nutzen in monetären Größen bewertet werden können, stellt die Kurve den resultierenden Gewinn dar. Solange der Grenznutzen größer als die Grenzkosten ist, steigt die Resultierende an, d.h., eine Erhöhung von x ist sinnvoll. Im Punkt x(opt) sind Grenznutzen und Grenzkosten gleich. Ab diesem Punkt ist es ökonomisch nicht sinnvoll, x weiter zu erhöhen. Wird x weiter erhöht, fällt die Resultierende wieder ab, da die Grenzkosten nun den Grenznutzen übersteigen, d.h. weitere Steigerungen von x werden nur mit einem unverhältnismäßig hohen Aufwand erreicht. Das Ziel eines Unternehmens muss es folglich sein, für seine Maßnahmen das optimale Ausmaß x zu ermitteln.

---

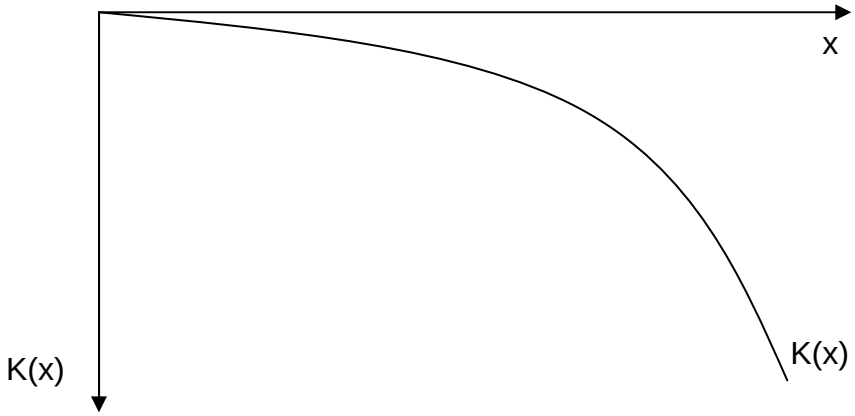
[23] Woll, 1996, S. 54

[24] Vgl. Brümmerhoff, 2001, S. 194.

[25] ebenda, S. 206

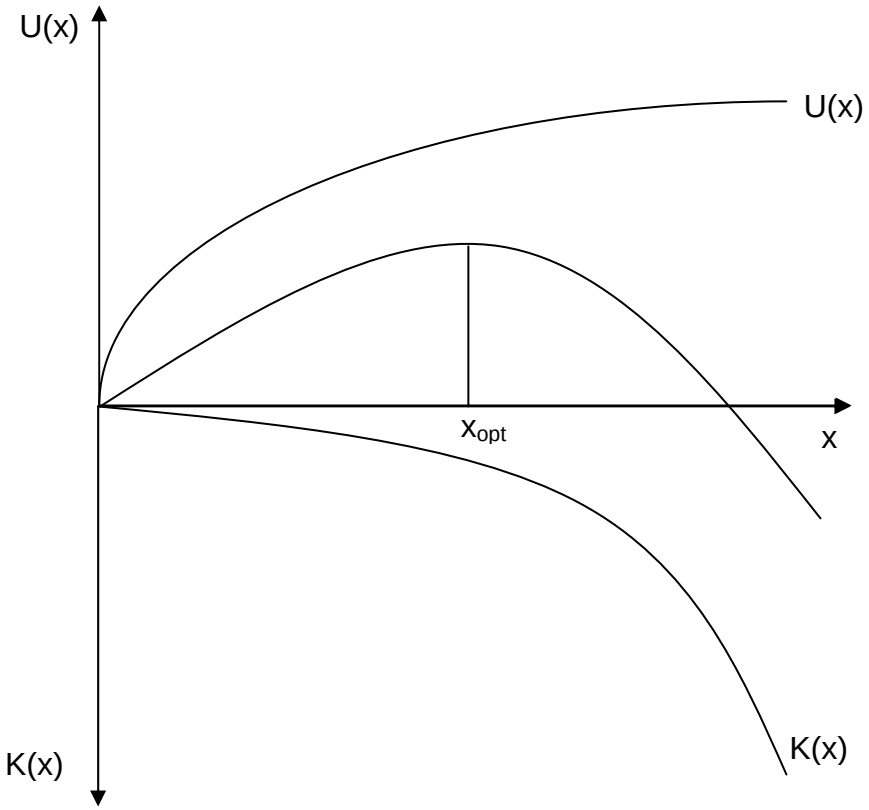
[26] Woll, 1996, S. 176

Abbildung 3:
Verlauf der Kostenkurve



Quelle: Eigene Darstellung

Abbildung 4:
Kosten-Nutzen-Verlauf mit Optimum (schematisch)



Quelle: Eigene Darstellung

Übertragen auf das Problem der Pay-TV-Piraterie könnte die Frage lauten: Wie hoch ist die optimale Intensität der Maßnahmen des Schwarzseher-Ausschlusses, die keine überproportional hohen Kosten im Verhältnis zum Nutzen des erreichten Ausschlusses verursacht?

2.3. Begriff des Pay-TV

Pay-TV, im Deutschen auch Bezahlfernsehen genannt, stellt eine bestimmte Finanzierungsform des Fernsehens dar. Pay-TV-Sender sind Unternehmen mit Gewinnerzielungsabsicht, die als Leistung Fernsehen gegen Entgelt anbieten.[27] Im Gegensatz zu den sogenannten Free-TV-Sendern, die sich im privaten Bereich vor allem mit Hilfe von Werbeeinnahmen, im öffentlich-rechtlichen Sektor zusätzlich noch durch Rundfunkgebühren finanzieren und für die Rezipienten, abgesehen von diesen Rundfunkgebühren, kostenlos sind,[28] generieren Pay-TV-Anbieter ihre Einnahmen in erster Linie aus Zuschauerentgelten.[29] Dabei beziehen die Rundfunkteilnehmer auf der Grundlage eines zivilrechtlichen Vertrags gegen Zahlung eines Entgeltes an den Pay-TV-Anbieter bestimmte Fernsehdarbietungen.[30] Eine zusätzliche Finanzierung durch Werbung ist jedoch nicht ausgeschlossen.[31]

Pay-TV ist ein Oberbegriff für verschiedene entgeltfinanzierte Fernsehformen. Diese unterscheiden sich in Abonnementfernsehen, auch als Pay-per-channel für einen Kanal bzw. Pay-per-package für ein Programmpaket bezeichnet,[32] Pay-per-view, Multichannel-pay-per-view bzw. Near-video-on-demand und Video-on-demand (siehe hierzu Abbildung 5). Beim Abonnementfernsehen entrichtet der Zuschauer ein in der Regel monatliches Entgelt an den Programmanbieter.[33] Im Gegenzug erwirbt er das Recht, alle Sendungen und Programme des abonnierten Kanals bzw. Programmpakets empfangen zu können. Der Programmablauf ist hierbei von der Senderseite vorgegeben. Letzteres gilt auch für das Pay-per-view-Verfahren, allerdings muss der Zuschauer nur für die Sendungen bezahlen, die er tatsächlich abruft. Beim Near-video-on-demand, auch als Multichannel-pay-per-view bezeichnet, erfolgt die Ausstrahlung der gleichen Sendung zeitversetzt auf verschiedenen Kanälen, so dass der Zuschauer zwischen verschiedenen Anfangszeiten einer bestimmten Sendung wählen kann und daher kaum noch an einen bestimmten Programmablauf gebunden ist. Beim Video-on-demand kann der Zuschauer eine gewünschte Sendung, die beim Anbieter auf einem zentralen Videoserver in digitaler Form gespeichert ist,

---

[27] Vgl. Pagenstedt, 1995, S. 2.

[28] Dietl, Franck, 1999, S. 11

[29] Vgl. Michaelsen, 1996, S. 5.

[30] Becker, 1992, S. 231

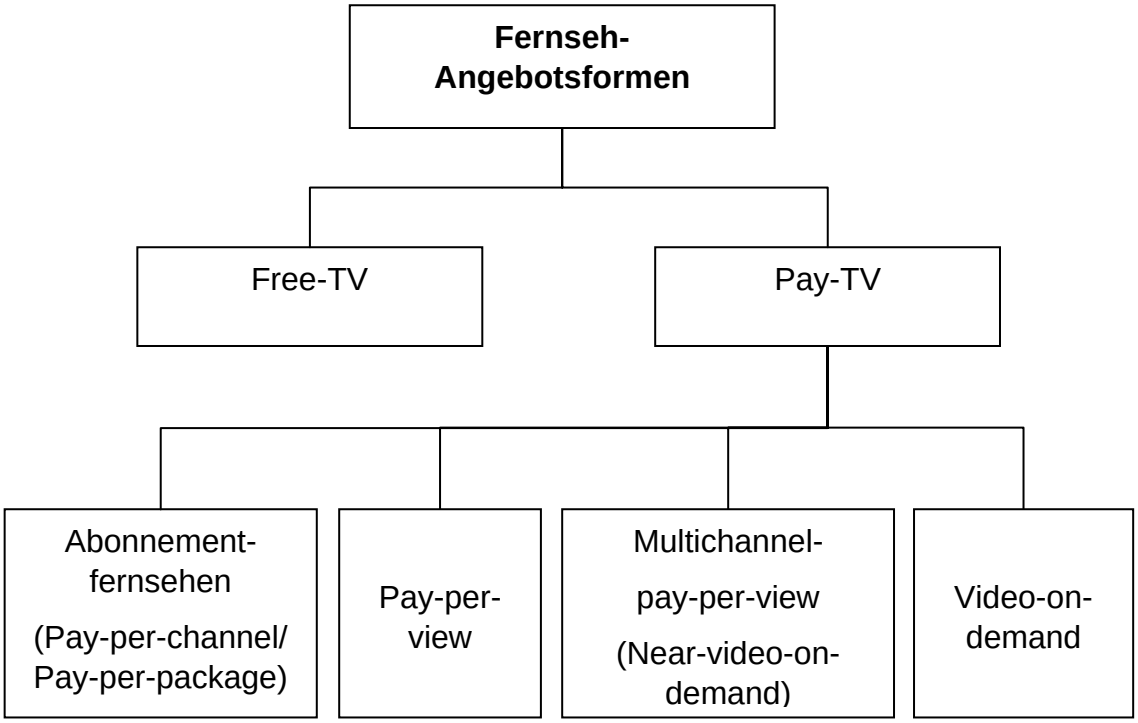
[31] Pagenstedt, 1995, S. 7

[32] o.V., o.J.(27)

[33] Pagenstedt, 1995, S. 2

jederzeit und unabhängig von anderen Nutzern abrufen.[34] Die Anforderung des Films bei der Abspielzentrale erfolgt hierbei über eine Telefonverbindung oder einen Rückkanal des Kabelanschlusses.[35] Gegenwärtig und in absehbarer Zukunft gibt es in Deutschland nur Verteil-Pay-TV in Form von Abonnements oder Pay-per-view.[36] Abruf-Pay-TV in Form von Video-on-demand-Services wird statt dessen über das Internet angeboten.[37]

Abbildung 5:
Fernseh-Angebotsformen



Quelle: Eigene Darstellung

Pay-TV spielt eine bedeutende Rolle in der Verwertungskette von Filmen. Die Aufführungsrechte eines Filmwerks werden nach der Kinoauswertung neben dem Video- bzw. DVD-Vertrieb zunächst an die Pay-TV-Stationen verkauft, erst später werden die Filme über das Free-TV ausgestrahlt.[38] Zwischen jedem Verwertungsschritt liegt ein gewisses Zeitfenster (daher wird in diesem Zusammenhang auch von „Windowing“ gesprochen), das eine größtmögliche kommerzielle Verwertung auf jeder der vier Verwertungsebenen gestattet.[39]

---

[34] Michaelsen, 1996, S. 5.

[35] Rother, 1994, S. 118.

[36] Koschnik, 2004.

[37] Bspw. bietet „t-online“ mit dem Angebot „t-online-vision“ Filme auf Abruf an.

[38] Vgl. Lenhardt, 1991, S. 4.

[39] Vgl. Abel, 1991, S. 41.

2.4. Pay-TV als bestimmte Güterart

2.4.1. Unterscheidung verschiedener Arten von Gütern

In den Wirtschaftswissenschaften gibt es eine Reihe verschiedener Unterscheidungsmethoden von Güterarten. Für die im folgenden angewandte, aus der Finanzwissenschaft stammende[40] Methode werden die Differenzierungskriterien „Rivalität im Konsum“ und „Ausschließbarkeit“ herangezogen.

Liegt Rivalität im Konsum vor, ist bei Nutzung eines Gutes durch ein Wirtschaftssubjekt die gleichzeitige Nutzung desselben Gutes durch alle anderen Wirtschaftssubjekte ausgeschlossen. Ein nicht-rivales Gut hingegen steht bei seiner Nutzung durch ein oder mehrere Wirtschaftssubjekte auch für alle anderen Wirtschaftssubjekte zur Verfügung, ist also gemeinschaftlich nutzbar.[41] Durch die Bereitstellung eines nicht-rivalen Gutes für einen weiteren Konsumenten entstehen keine weiteren Kosten, die Grenzkosten sind null.[42] Das Kriterium der Ausschließbarkeit zielt auf die Möglichkeit ab, kooperations- oder zahlungsunwillige Mitglieder einer Nutzergruppe auf ökonomische oder technische Weise vom Konsum eines bestimmten Gutes auszugrenzen. Die Ausschließbarkeit stellt damit einen wirksamen Sanktionsmechanismus dar, der es gestattet, die Nutzung eines Gutes nur unter bestimmten Bedingungen, z.B. gegen Zahlung eines Entgeltes, zu erlauben.[43]

Aufgrund dieser Kriterien lassen sich vier verschiedene Güterarten differenzieren (siehe Abbildung 6): private Güter, Clubgüter (auch als Mautgüter bezeichnet), Allmendegüter und (reine) öffentliche Güter. Private Güter sind rival im Konsum, da bei der Nutzung durch eine Person allen anderen die Möglichkeit genommen wird, das Gut ebenfalls zu nutzen. Gleichzeitig können Personen von der Nutzung ausgeschlossen werden. Ein Beispiel für ein privates Gut ist ein Brötchen. Der Eigentümer des Brötchens kann die Herausgabe desselben verweigern und damit alle anderen vom Konsum ausschließen. Gleichzeitig ist das Brötchen rival im Konsum, denn beim Verzehr kann das gleiche Brötchen nicht auch noch durch andere Personen konsumiert werden.

Als Clubgüter werden solche Güter bezeichnet, die dem Ausschlussprinzip unterliegen, jedoch nicht rival im Konsum sind. Eine Kinovorstellung in einem geschlossenen Saal ist nur denjenigen zugänglich, die zuvor ein Ticket gekauft haben. All denen, die kein Ticket besitzen, bleibt der Film verwehrt. Trotz des Konsums des Films durch einen Zuschauer bleibt allen anderen Zuschauern die Möglichkeit erhalten, den Film ebenfalls anzuschauen, es liegt also keine Rivalität im Konsum vor.

Allmendegüter sind Güter, bei denen Rivalität im Konsum vorliegt, jedoch die Möglichkeit einer Ausschließbarkeit nicht besteht. Fische in einem öffentlichen

---

[40] Hansmeyer, Kops, 1998, S. 5

[41] Brümmerhoff, 2001, S. 94

[42] Stiglitz, Schönfelder, 2000, S. 117

[43] Brümmerhoff, 2001, S. 94

Gewässer sind solche Allmendegüter. Wird ein Fisch von einem Fischer gefangen, kann derselbe Fisch nicht auch noch von einem anderen Fischer gefangen werden. Somit ist das Gut Fisch rival im Konsum. Da der Fisch in dem öffentlichen Gewässer niemandem gehört, kann niemand ausgeschlossen werden, den Fisch zu fangen, daher existiert hier das Ausschließbarkeitsprinzip nicht.

Reine öffentliche Güter weisen weder eine Rivalität im Konsum noch die Möglichkeit des Ausschlusses auf. Ein typisches Beispiel für ein öffentliches Gut ist die Landesverteidigung. Einzelne Einwohner können vom Schutz durch die Verteidigungsmaßnahmen nicht ausgeschlossen werden. Gleichzeitig ist es für keinen Einwohner nachteilig, dass ein beliebiger anderer Einwohner ebenso von der Landesverteidigung profitiert. Sowohl Allmende- als auch öffentliche Güter sind aufgrund der Nicht-Ausschliessbarkeit für jeden frei zugänglich und kostenlos.[44]

Abbildung 6:
Unterscheidung von Güterarten

		Rivalität im Konsum	
		Ja	Nein
Ausschließbarkeit	Ja	Private Güter (z.B. Kleidung, Nahrungsmittel)	Clubgüter (Kinovorstellung, *Pay-TV?*)
	Nein	Allmendegüter (Hochseefischgründe)	Reine öffentliche Güter (Innere und äußere Sicherheit)

Quelle: Eigene Darstellung

2.4.2. Einordnung von Pay-TV als bestimmte Güterart

Bei Nutzung eines Pay-TV-Angebots durch einen Kunden bleibt der Konsum der Sendung auch für alle anderen Zuschauer ohne Beeinträchtigung möglich. Die Eigenschaft der Nichtrivalität im Konsum wird daher offensichtlich erfüllt.[45]

---

[44] Mankiw, 2004, S. 247

[45] Dietl, Franck, S. 3. Unter Umständen kann jedoch auch eine begrenzte Konsumrivalität angenommen werden, da mit der Ausweitung des Rezipientenkreises von Rundfunkprogrammen eine Verringerung des Nutzens für den einzelnen Rezipienten verbunden sein kann. Siehe hierzu: Hansmeyer, Kops, 1998, S. 6. Ebenso kann bis zu einer bestimmten Rezipientenzahl eine Ausweitung auch nutzensteigernd wirken, da es z.B. eine Auswahl an Gesprächspartnern über einen zuvor gesehenen Film gibt. Vgl. hierzu Heinrich, 1999, S. 30.

Den Ausschluss von Zuschauern, die nicht bereit sind, Geldleistungen für das empfangene Programm zu erbringen, beabsichtigen die Pay-TV-Anbieter durch technische Maßnahmen zu erreichen. Aufgrund der Existenz und Anwendung der technischen Ausschlusseinrichtungen wird Pay-TV oft als ein Beispiel für ein Clubgut aufgeführt. Sofern diese Maßnahmen wirksam sind und jeden Nichtberechtigten vom Konsum des zahlungspflichtigen Programms ausschließen, ist das Gut Pay-TV tatsächlich als Clubgut einzustufen. In praxi haben Pay-TV-Anbieter jedoch mit Schwarzsehern zu kämpfen, die die Ausschlussmaßnahmen überlisten. Ob Pay-TV daher als eindeutiges Clubgut kategorisiert werden kann, wird sich in der folgenden Untersuchung herausstellen.

3. Das Schwarzseher-Problem aus Sicht der Pay-TV-Anbieter

3.1. Pay-TV-Piraterie

Pay-TV-Anbieter sind auf Einnahmen durch die Zuschauer angewiesen. Die Verschlüsselung des ausgestrahlten Programms soll sicherstellen, dass nur solche Zuschauer die Sendungen in guter Qualität empfangen können, die durch entsprechende Zahlungen, wie die monatlichen Abonnement-Gebühren oder Abrufgebühren beim Pay-per-view, dazu berechtigt sind. Alle anderen sollen von der Nutzung ausgeschlossen werden.[46] Diejenigen Zuschauer, die die codierten Programme bei sich entschlüsseln, ohne das entsprechende Entgelt an die Pay-TV-Anbieter abzuführen, sind sogenannte Schwarzseher. Dieses Verhalten ist vergleichbar mit dem eines Trittbrettfahrers, auch als „free rider" bezeichnet.[47] Ein free rider erlangt den Nutzen eines nicht-freien Gutes, ohne dafür zu bezahlen.[48] Die Tatsache, dass die Aussendung und damit auch der Empfang eines Fernsehsignals nur flächendeckend und nicht punktgenau erfolgt[49], motiviert die Pay-TV-Piraten, eine Lösung zu finden, wie sie ein empfangenes codiertes Signal entschlüsseln und damit den Nutzen des Gutes Pay-TV erlangen können, ohne dabei die Gebühren an den Pay-TV-Anbieter leisten zu müssen.

Schwarzsehen ist eine Form der audiovisuellen Piraterie. Dies ist die illegale Nutzung von audiovisuellen Werken, ohne dazu berechtigt zu sein. Piraterie im Bereich des Bezahlfernsehens ist die unberechtigte Entschlüsselung codierter Fernsehsignale.[50] Unter Piraten werden diejenigen Personen verstanden, die an den Tätigkeiten zur Ermöglichung oder Durchführung der unberechtigten Nutzung von Multimediainhalten beteiligt sind.[51] Dazu gehören im Falle der Pay-TV-Piraterie die Hersteller der für das Schwarzsehen benötigten Umgehungslösungen, auch als Hacker bezeichnet, die Dealer als die Distributoren dieser Lösungen sowie deren Nutzer, die Schwarzseher selbst.

Kein Verschlüsselungssystem ist dauerhaft vor Piraterie geschützt.[52] Früher oder später wird jeder Schutzmechanismus überwunden werden können. In Europa und darüber hinaus sind Tausende Hacker damit beschäftigt, verschlüsselte Signale zu knacken.[53] Die zum illegalen Entschlüsseln benötigte Computertechnik kann zu moderaten Preisen erworben werden. Im Internet

---

[46] Vgl. Tetzner, 1991, S. 19.

[47] Zum Problem der „free rider" siehe auch Mankiw, 2004, S. 248f., Brümmerhoff, 2001, S. 100ff., Stiglitz, Schönfelder, 1989, S. 114f. u.a.

[48] Mankiw, 2004, S. 248

[49] Die bei Satelliten verwendeten Antennen ermöglichen üblicherweise den Empfang eines abgestrahlten Programms in ganz Europa. Siehe hierzu: Freyer, o.J.

[50] Vgl. o.V., o.J.(25).

[51] Vgl. Lievaart, 2001, S. 1

[52] Dinsel, 1991, S. 10

[53] o.V., o.J. (20)

werden die neuesten Informationen über Knackmethoden schnell verbreitet und in speziellen Foren neue Ideen zur Überwindung der Verschlüsselungen ausgetauscht.[54] Auf Tausenden von Webseiten im Internet werden Hacker-Software, Zugangscodes und Beschreibungen für den illegalen Zugang zu Pay-TV bereitgestellt. Auch Piraten-Smartcards werden auf diesen Webseiten angeboten.[55] Potentielle Schwarzseher werden kostengünstig mit E-Mails angesprochen, in denen die neuesten illegalen Zugangsmethoden angepriesen werden.[56] Die Süddeutsche Zeitung berichtete, dass pro Jahr 1,25 Millionen Internetnutzer Pay-TV-Hackerseiten aufrufen.[57] Hinzu kommen Berichte diverser Computerzeitschriften, die regelmäßig Anleitungen und Tipps für den gebührenfreien Empfang von Abo-Sendern geben.[58] Selbst im Fachhandel kann man erfahren, wie man sich kostenpflichtige Programme schwarz auf den eigenen Bildschirm holen kann. Stichproben haben ergeben, dass fast jeder zehnte Premiere-Händler eindeutige Empfehlungen für die Beschaffung von Piratenkarten gab, einige von ihnen boten diese Karten sogar selbst an.[59] Gegenwärtig erzeugen vor allem in Frankreich mit Chipsätzen ausgestattete Decoderboxen Besorgnis, die in Kombination mit bestimmter Software die illegale Decodierung von Pay-TV ermöglichen und zunehmend im Einzelhandel zu erwerben sind. Die dramatische Entwicklung in Frankreich hinsichtlich der Verfügbarkeit von leistungsfähigem Piraterie-Equipment gilt als beispielhaft für die zukünftige Entwicklung der Piraterie in ganz Europa, die von Experten als beängstigend bezeichnet wird.[60]

Pay-TV-Piraterie tritt in verschiedenen Formen auf. Bei Hackern und Schwarzsehern kann es sich um einzelne unabhängige Technikfreaks handeln, oft stecken hinter den Piraterie-Aktivitäten jedoch professionelle und gut organisierte Banden.[61] Sie werden vor allem durch hohe Gewinnaussichten angelockt, denen nur geringe persönliche Risiken aufgrund nicht ausreichender Gesetze bzw. Vollstreckungsmöglichkeiten gegenüberstehen.[62] Gründe für das Schwarzsehen liegen jedoch nicht nur im finanziellen Bereich. Oft gibt es für die Zuschauer eines Landes, obwohl sie bereit sind, die Gebühren zu entrichten, keine legale Möglichkeit, ein bestimmtes ausländisches Pay-TV-Programm zu abonnieren, auch wenn sie das Fernsehsignal empfangen können.[63] Auch die

---

[54] Ein solches deutschsprachiges Forum ist z.B. hier zu finden: http://www.spinnesboard.de/vb/ (Stand: 05.11.2004).

[55] o.V., o.J.(20)

[56] Lievaart, 2001, S. 1

[57] o.V., 2002(11)

[58] Vgl. o.V., 2002(1).

[59] o.V., 2002(11)

[60] o.V., 2004(5)

[61] Janz, 2002

[62] o.V., 2003(5)

[63] o.V., 2003(4)

1989 verabschiedete EU-Richtlinie „Fernsehen ohne Grenzen“[64] kann dies nicht ändern, da ihr diverse Urheberrechte von Herstellern, das Recht auf geistiges Eigentum und die Privatautonomie, das Recht auf freie Vertragspartnerwahl, entgegenstehen.[65] Hintergrund sind die Ausstrahlungsrechte, die ein Pay-TV-Sender oft nur für ein bestimmtes Land erwirbt. Durch die vertragliche regionale Limitierung seines Angebots kann ein Sender die Ausstrahlungsrechte deutlich billiger erwerben. Im Anschluss daran dürfen sich in- und ausländische Sender nicht in die Quere kommen. Beispielsweise werden die Satellitenausstrahlungen des österreichischen Senders ORF auf Druck durch die Rechteinhaber und Sender in Deutschland nur noch in verschlüsselter Form gesendet, da ansonsten Filme in Deutschland bereits vor der Ausstrahlung durch die einheimischen Sender zu sehen wären.[66] Da der Abschluss eines gültigen Abonnementvertrages meistens an einen inländischen Wohnsitz bzw. an eine gültige Aufenthaltsbescheinigung des Kunden gebunden ist und insbesondere für Ausländer einen hohen zeitlichen Aufwand erfordert, sehen ausländische Interessenten die einzige Möglichkeit in einem illegalen Zugang zu den gewünschten Programmen.[67] Die Ausgaben der Zuschauer fließen dann den Pay-TV-Piraten und nicht den Sendern bzw. Rechteinhabern zu.[68]

Eine weitere Ursache für das Schwarzsehen ist, dass die verschiedenen Pay-TV-Anbieter sich unterschiedlicher Verschlüsselungssysteme bedienen. Ein Kunde, der die Angebote mehrerer Pay-TV-Sender nutzen möchte, muss daher häufig unterschiedliche Zugangs-Module kaufen, welche mit relativ hohen Kosten zwischen 50,- und 200,- Euro zu Buche schlagen. Für einige Verschlüsselungssysteme gibt es sogar keine derartigen Module, so dass statt. dessen eine zusätzliche Decoderbox angeschafft werden muss.[69] Die illegale Umgehung des Zugangs zu den Programmen erscheint den Schwarzsehern dann als die günstigere Alternative.

Geschädigte der Pay-TV-Piraterie sind die Pay-TV-Sender, deren zahlende Kunden, Rechteinhaber, die Händler der legalen Zugangstechnik und der Staat. Für die Sender besteht durch die entgangenen Abonnenten-Entgelte die Gefahr, dass sie langfristig nicht genügend Einnahmen erzielen können, um ihr Programm kostendeckend auszustrahlen.[70] Zusätzlich müssen sie laufend hohe Geldbeträge für aktuelle Verschlüsselungstechniken und weitere Bekämpfungsmaßnahmen wie z.B. die Verfolgung von Pay-TV-Piraten ausgeben, um gegen die Schwarzseher gefeit zu sein. In Folge dieser Verluste müssen die Kunden

---

64 Richtlinie 89/552/EWG des Rates vom 3. Oktober 1989 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Ausübung der Fernsehtätigkeit

65 Meyer, Sprotte, 2003b, S. 120

66 Posewang, 2004, S. 39

67 Meyer, Sprotte, 2003b, S. 120

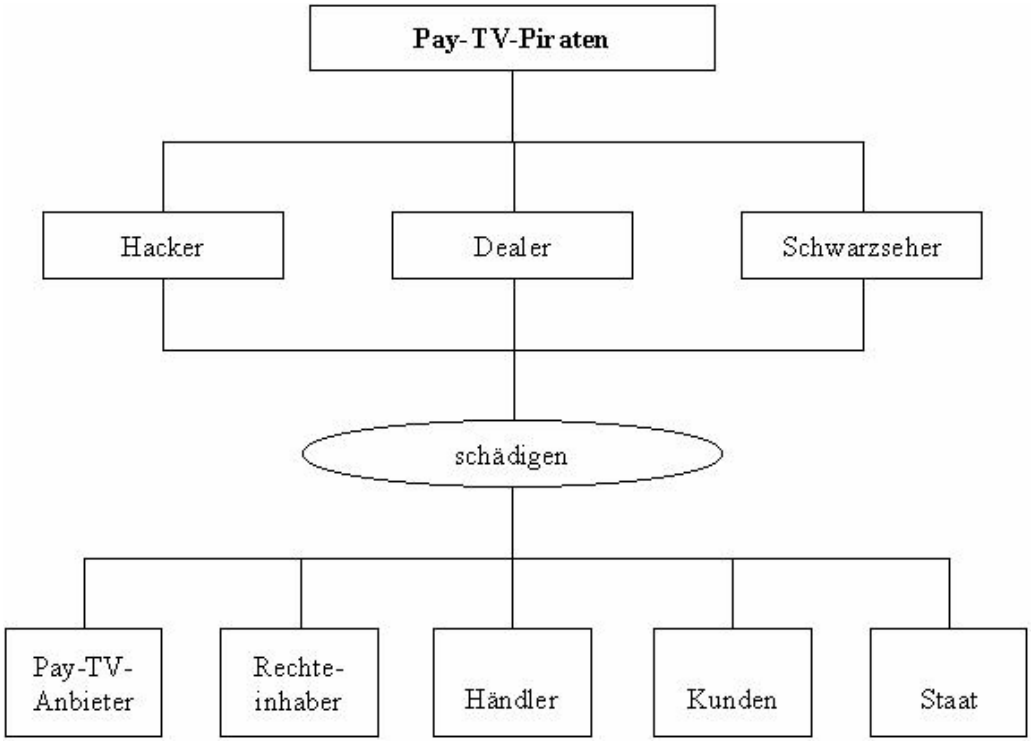
68 o.V., 2003(3), S. 23

69 Meyer, Sprotte, 2003b, S. 120

70 Vgl. Tetzner, 1991, S. 23.

höhere Gebühren bezahlen oder sich mit einem kostengünstigeren Programm bzw. eingeschränktem Service zufrieden geben. Ebenso betroffen sind die Inhaber der Urheberrechte bzw. Verwertungsrechte an den ausgestrahlten Filmwerken, da der tatsächliche Zuschauerkreis größer ist als der mit dem Pay-TV-Sender vertraglich vereinbarte und den Rechteinhabern daher Einnahmen für die Ausstrahlung ihrer Werke entgehen. Händler des legalen Pay-TV-Zugangsequipments wie Decoderboxen, CI-Module oder Smartcards müssen Umsatzeinbußen verzeichnen, da illegale Zugänge diese Geräte überflüssig machen oder statt dessen entsprechendes Piraten-Equipment auf dem Schwarzmarkt besorgt wird.[71] Letztlich wird auch der Staat geschädigt, da ihm Steuerausfälle sowohl auf der Seite der Schwarzseher, die keine Steuern für den Kauf des Programms abführen, als auch auf der Seite des Senders entstehen, da aufgrund von Umsatzausfällen und des niedrigeren zu versteuernden Gewinns entsprechend weniger Steuern anfallen.[72]

Abbildung 7:
Täter und Opfer der Pay-TV-Piraterie



Quelle: Eigene Darstellung

[71] o.V., o.J.(20)

[72] o.V., 2003(4)

Im Folgenden wird analysiert, welche Bedeutung das Problem der Schwarzseher für die Fernsehsender hat, welche Auswirkungen sich daraus ergeben, welche Maßnahmen durch Pay-TV-Sender ergriffen werden müssen und mit welchen Kosten das Schwarzseher-Problem verbunden ist.

3.2. Ökonomische Auswirkungen des Schwarzsehens

Das illegale Entschlüsseln von Pay-TV ist ein weit verbreitetes Phänomen. Allein das Knacken des deutschen Pay-TV-Senders Premiere nahm zwischenzeitlich das Ausmaß eines Volkssports ein.[73] Ist eine Verschlüsselung erst einmal geknackt, kann die Anzahl der Schwarzseher beträchtlich sein. Beispielsweise schätzte Premiere im Jahr 2003, bevor das Unternehmen seine Verschlüsselungstechnik ausgetauscht hat, die Anzahl der Schwarzseher, die sich mit illegalen Smartcards Zugang zum Premiere-Programm verschafften, auf 1,7 Millionen.[74]

Das Knacken der Verschlüsselungscodes und das damit einhergehende Problem der Schwarzseher ist mit schwerwiegenden wirtschaftlichen Konsequenzen für die Pay-TV-Anbieter verbunden. Ein Gutachten des Technischen Überwachungsvereins (TÜV) vom September 2000, welches von der Münchener Kirch-Gruppe in Auftrag gegeben worden war, sagte Premiere einen wirtschaftlichen Schaden durch Piraterie bis zum Jahr 2004 in Höhe von 800 Millionen Euro voraus.[75] Allein im Jahr 2000 sind Premiere nach den TÜV-Schätzungen durch die Möglichkeit des Schwarzsehens rund 90.000 potentielle Kunden entgangen.[76] Nach Auffassung des Premiere-Chefs Kofler könnte sein Unternehmen schon längst Gewinne erzielt haben, falls damals nur ein Teil der Schwarzseher zu seinen regulären Kunden gezählt hätte.[77] Die Optionen der Pay-TV-Piraterie halten nicht nur potentielle Kunden von dem Abschluß eines regulären Abonnements ab, sondern können auch zu massiven Rückgängen der Bestandskunden führen, wie sich am Beispiel des skandinavischen Senders Viasat belegen läßt. Viasat hat bereits seit einigen Jahren mit dem Pirateriepoblem zu kämpfen. Für einige seiner Kanäle, die im D2-MAC-Standard ausgestrahlt und mit Eurocrypt verschlüsselt werden, existierten sogar mehr illegale als legale Smartcards. Der Sender verzeichnete in Folge dessen mehrfach Einbrüche bei den Abo-Zahlen.[78]

---

[73] o.V., 2002(1).

[74] Schmerer, 2003; die Angaben schwanken, andere Quellen verweisen ebenfalls auf Premiere-Angaben, in denen die Anzahl der Schwarzseher damals auf eine bis anderthalb Millionen oder auch ein bis zwei Millionen Haushalte geschätzt wurde; vgl. hierzu: Pötzsch, 2003, Fiutak, 2003, Goedecke, Hofmeir, 2003c, S. 23.

[75] o.V., 2002(11)

[76] Jakobs, 2000

[77] o.V., 2002(11)

[78] Hagedorn, 2004a, S. 21

Der Rückgang zahlungsbereiter Kunden aufgrund illegaler Zugangsmöglichkeiten führt zu einem Verlust des Absatzpotentials. Damit einher geht eine Steigerung der Akquisitionskosten[79] sowie der Fixkosten je zahlendem Abonnent, da die anfallenden Kosten nur noch auf weniger (Abonnenten-) Köpfe verteilt werden können. Fixkosten, also von der Anzahl der Abonnenten unabhängig anfallende Kosten, spielen in der Kostenbilanz eines Pay-TV-Senders eine bedeutende Rolle. Beispielsweise entstanden im Jahr 2002 bei Premiere Kosten für das Programm in Höhe von 697,3 Millionen Euro. Für Technik und Übertragung, deren Kosten auch zum überwiegenden Teil fix sein dürften, fielen Kosten in Höhe von 118,6 Millionen Euro an. Beide Posten machten zusammen 60,9 Prozent der gesamten Kosten (inkl. Abschreibungen) aus.[80] Den Pay-TV-Sendern droht ein Dilemma: Werden die Kosten in Form höherer Gebühren an die Kunden weitergegeben, führt dies zu einem erneuten Rückgang an Abonnenten, da bei einigen Kunden die persönliche maximale Zahlungsbereitschaft für das Pay-TV-Angebot durch die Preiserhöhung überschritten wird. Dieser Rückgang an Abonnenten erhöht wiederum die Fixkosten pro Abonnent. Werden die erhöhten Kosten jedoch nicht an die Kunden weitergegeben, sondern vom Pay-TV-Sender selbst getragen, verursacht dies bei dem Sender einen Gewinnrückgang bzw. einen höheren Verlust. Um die Kosten zu senken, werden Einsparpotentiale im Inhalte-Bereich durch den Einkauf billigerer, jedoch meist auch qualitativ schlechterer Fernsehsendungen realisiert. Dies schürt bei den Kunden Unzufriedenheit, ihre Zahlungsbereitschaft für das nun geringerwertige Angebot sinkt. Einige der Abonnenten werden in der Folge kündigen. Dadurch sinken die Einnahmen weiter, erneute Einsparmaßnahmen müssen getroffen werden (siehe Abbildung 8).

Hinzu kommen zwei weitere Faktoren: Zum einen werden Pay-TV-Abonnenten bei zunehmender Anzahl von Schwarzsehern mit der Frage konfrontiert, warum sie selbst überhaupt bezahlen, während viele andere Zuschauer die selben Sendungen auch ohne die entsprechenden Gebührenleistungen empfangen können. Mit steigender Anzahl an Schwarzsehern kann sich daher auch die Zahlungsmentalität der ehrlichen Kunden zunehmend verändern, so daß auch sie zu illegalen Zuschauern werden. Zum anderen sind auch die Rechteinhaber bei einer hohen Anzahl von Schwarzsehern nicht mehr bereit, ihre Filmwerke den Pay-TV-Sendern zur Verfügung zu stellen, da auch sie um Einnahmen betrogen werden.[81] Unterbleiben wirksame Bemühungen gegen die Piraterie seitens des Pay-TV-Senders, kann dies die Inhaber dieser Rechte dazu veranlassen, dem Sender die Ausstrahlungsrechte zu verweigern, was wiederum eine Quantitäts- und Qualitätsverschlechterung des Programmangebots zur Folge haben kann. Dies vermindert dann erneut die Zahlungsbereitschaft der Kunden,

---

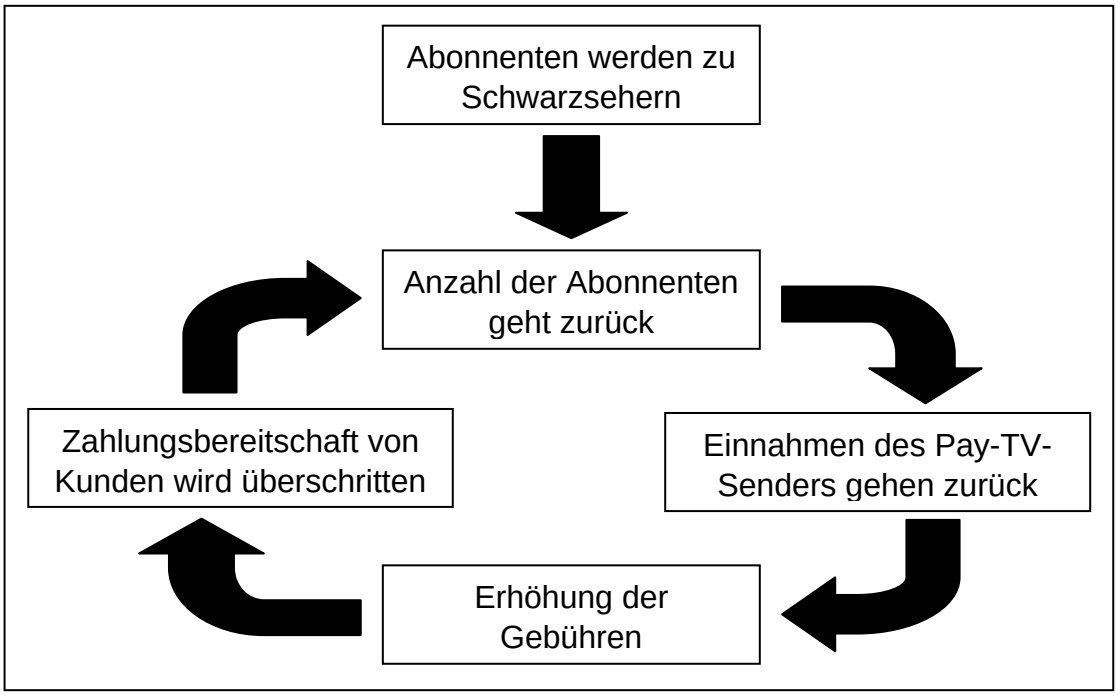
[79] Haas, 1991, S. 36. Die Akquisitionskosten pro Neuabonnent betrugen z.B. für Premiere im Jahr 2004 184,-€. Siehe hierzu: o.V., 2005(1).

[80] o.V., 2003(2), S. 11

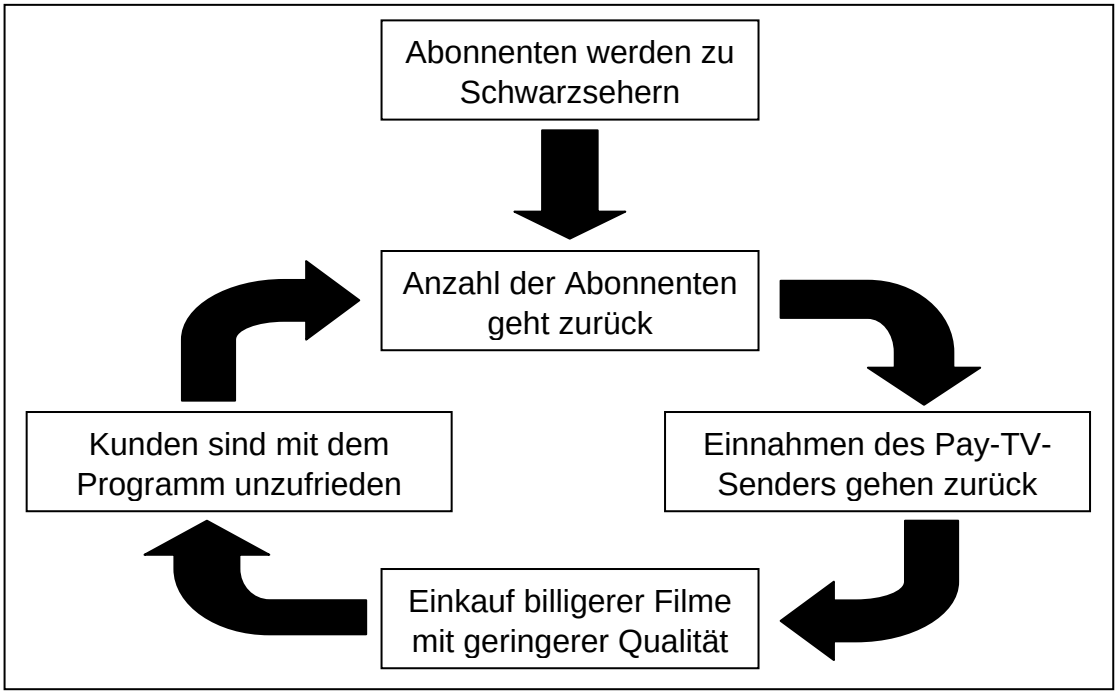
[81] Vgl. Lievaart, 2001, S. 1. Die Entlohnung der Rechteinhaber erfolgt häufig aufgrund der erwarteten Zuschauerzahlen, siehe hierzu: o.V., 2003(3), S. 23.

die Abonnentenzahlen gehen zurück, die Einnahmen der Sender fallen, usf. Durch die geringeren Einnahmen steht dann in der Folge auch immer weniger Geld zur Verfügung, um wirksame Maßnahmen gegen Schwarzseher, z.B. In-

Abbildung 8:
Folgen des Schwarzsehens für Pay-TV-Sender



Quelle: Eigene Darstellung



vestitionen in Verbesserungen der Verschlüsselungssysteme, zu ergreifen. Am Ende dieser Entwicklung stände der Konkurs der Pay-TV-Anbieter.[82] Sie sind daher gezwungen, in Maßnahmen zu investieren, die die Anzahl der Schwarzseher und die damit verbundenen Konsequenzen minimieren.

Allein in einer Hinsicht erweisen sich Schwarzseher als wenig problematisch: Pay-TV-Sender können zur Generierung von Einnahmen auch Werbung ausstrahlen. Beispielsweise werden bei Premiere vor und nach Spielfilmen Werbespots gesendet.[83] Typischerweise hängen die Werbepreise von der Reichweite ab, also von der Anzahl der Zuschauer, die diese Werbung empfangen können. Dabei spielt es keine Rolle, ob es sich bei den Zuschauern um zahlende Kunden oder Schwarzseher handelt. Je mehr erreichbare Zuschauer es gibt, desto höher sind die Werbepreise und desto höher sind die daraus resultierenden Einnahmen. In diesem Falle würde ein Pay-TV-Sender sogar von einer höheren Zahl an Schwarzsehern profitieren, da diese die Werbereichweite erhöhen. Premiere beabsichtigt zum Beispiel, mit Reklame bis zu fünf Prozent des Umsatzes zu generieren.[84] Bei einem Umsatz von 984,8 Millionen Euro im Jahr 2004[85] entspräche dies einem Betrag von 49,24 Millionen Euro im Jahr. Die Einnahmengenerierung durch Werbung kann die Sender daher dazu bewegen, von der Verfolgung der Schwarzseher abzusehen. Dieser Gedanke sei hier allerdings nur am Rande erwähnt, da sich diese Arbeit auf Pay-TV-Anbieter bezieht, die sich nicht oder nur zu einem unerheblichen und damit die Schwarzseherbekämpfung nicht beeinflussenden Teil aus Werbeeinnahmen finanzieren.

3.3. Die Notwendigkeit eines Verschlüsselungssystems

Die Codierungstechnik ist für die Anbieter von Pay-TV von außerordentlicher Bedeutung, da diese das ausgestrahlte Programm, die Geschäftsgrundlage des Senders, vor unberechtigtem Empfang schützen soll.[86] Um innerhalb eines bestimmten Verbreitungsgebietes, in dem das ausgestrahlte Fernsehprogramm prinzipiell empfangbar ist, nur den zahlenden und damit berechtigten Kunden den Zugang zu ermöglichen, muss mit technischer Hilfe ein Ausschluss der Nichtberechtigten erfolgen. Hierfür wird ein Zugangskontrollsystem, ein sogenanntes Conditional-Access-System (CA-System oder CAS) angewendet, welches dafür sorgt, dass die Nutzer nur mit einer legalen Zugangsberechtigung Zugriff erhalten.

Die CAS-Technik macht es erforderlich, dass der Zuschauer über eine Decoderbox verfügt, die entweder ein Conditional-Access-Modul (CA-Modul oder

---

[82] Pötzsch, 2002

[83] Weidner, 2003

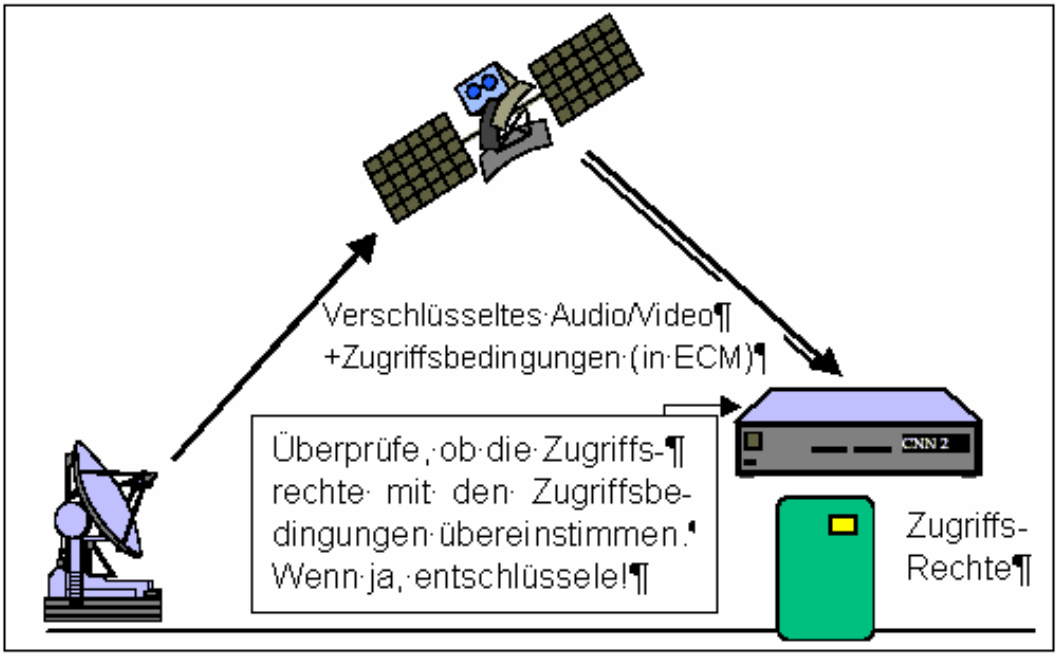
[84] ebenda

[85] o.V., 2005(1)

[86] Michaelsen, 1996, S. 38

CAM) bereits integriert hat oder über ein Common-Interface[87] (CI-Schnittstelle) verfügt, an die ein externes CA-Modul angeschlossen werden kann. Für den Empfang von Pay-TV funktioniert das CA-Modul des Zuschauers nur dann, wenn der Pay-TV-Sender eine entsprechende Verschlüsselung benutzt und der Zuschauer die richtige Smartcard[88] besitzt[89]. Mit dem Fernsehsignal in codierter Form werden die Daten der Empfangsberechtigung der einzeln adressierbaren Kunden übertragen. Smartcards, die den autorisierten Kunden durch den Pay-TV-Anbieter zur Verfügung gestellt und in den Decoder gesteckt werden, können die Berechtigungssignale entschlüsseln und an den Decoder weitergeben.[90] Das Smartcard-System hat sich in der Vergangenheit bewährt und wird mit jeder folgenden Entwicklungsstufe raffinierter.[91]

Abbildung 9:
Funktionsweise von Conditional Access



Quelle: nach Schwenk, o.J.

---

87 Ein Common-Interface ist eine herstellerunabhängige Schnittstelle, an die eine PCMCIA-Steckkarte, wie z.B. ein CI-CAM zum Decodieren von Pay-TV-Signalen, angeschlossen werden kann. Siehe hierzu: o.V., o.J.(7).

88 Eine Smartcard ist eine eigenständige Rechnereinheit im Scheckkartenformat mit Speicher, Prozessor und Kommunikationsschnittstelle, auf der kundenspezifische Zugangsdaten enthalten sind. Siehe hierzu: o.V., o.J.(19).

89 Vgl. Goedecke, Hofmeir, 2003b, S. 36; bei einigen Verschlüsselungssystemen wird keine zusätzliche Smartcard benötigt, hier genügt ein geeignetes und freigeschaltetes CA-Modul bzw. ein entsprechender Receiver.

90 Vgl. Pagenstedt, 1995, S. 9.

91 Posewang, 2004, S. 38

3.3.1. Funktionsweise der Verschlüsselungstechnik

Um auf eine besonders effektive Verschlüsselung zurückgreifen zu können, übertragen Pay-TV-Anbieter ihre Sendungen mittels digitaler Signale. Durch die digitale Technik lässt sich gegenwärtig der höchste Grad an Verschlüsselungssicherheit erreichen.[92] Zudem bietet sie den Vorteil, dass im Gegensatz zu den früheren analogen Verfahren keine Verschlechterung der Bildqualität eintritt. Außerdem können relativ schnell Verschlüsselungsänderungen durchgeführt werden, sobald die Verschlüsselungssicherheit nicht mehr gegeben ist.[93]

Technisch basieren die CA-Systeme auf den Prinzipien der Verwürfelung (Scrambling) bzw. Verschlüsselung (Encryption) des DVB[94]–Transportstroms. Die technische Abfolge lautet dabei: Verwürfelung, Verschlüsselung, Übertragung, Entschlüsselung, Entwürfelung.[95] Die Verwürfelung bewirkt das Vertauschen von Bitfolgen der Signale für Bild oder/und Ton nach einem europaweit[96] standardisierten Verschlüsselungsalgorithmus.[97] Anschaulicher bedeutet dies, die Einsen und Nullen des Digitalsignals[98] werden vertauscht oder leere Bitfolgen hinzugefügt.[99] Dabei muss die Verwürfelung so komplex sein, dass sie durch die automatische Fehlerkorrektur des Empfängers nicht bereits decodiert werden kann und die Weitergabe des Signals verweigert wird. Damit das Signal beim Empfänger zu einem erkennbaren Bild wird, muss die Verwürfelung rückgängig gemacht werden. Hierfür muss der Empfänger über einen bestimmten technischen Schlüssel verfügen (siehe Abbildung 10). Die meisten Systeme verfügen sogar über zwei Schlüssel: zum einen die Zugangsberechtigung auf der Empfängerseite in Form der Smartcard, die der Kunde bei Vertragsabschluss vom Pay-TV-Anbieter erhält und in das Kartenlesegerät des Receivers oder des CA-Moduls steckt, zum anderen in Form elektronischer Passwörter, die von der Sendezentrale zusammen mit dem Datenstrom des Fernsehsignals verschickt werden. Die Entwürfelung des Signals ist erst dann möglich, wenn die Passwörter durch die auf der Smartcard gespeicherten Daten erkannt werden.[100]

---

92 Dinsel, 1991, S. 10

93 Schlomski, o.J.

94 DVB ist die Abkürzung für „Digital Video Broadcasting“ und bezeichnet ein standardisiertes Verfahren zum Übertragen digitaler Inhalte durch digitale Technik. Siehe hierzu z. B. im Internet, URL: http://www.computerbase.de/lexikon /Digital_Video_Broadcasting oder www.dvb.org (Stand: 03.01.2005).

95 Freyer, o.J.

96 ebenda

97 Ein Verschlüsselungsalgorithmus ist eine mathematische Funktion zur Ver- und Entschlüsselung. Siehe hierzu: o.V., 1999, S. 3.

98 Das digitale Signal kann innerhalb eines festen Zeittaktes zwei Werte aufweisen, die i.d.R. mit 0 oder 1 gekennzeichnet werden. Siehe hierzu z.B. im Internet: http://www.bullhost.de/d/digital.html (Stand: 03.01.2005).

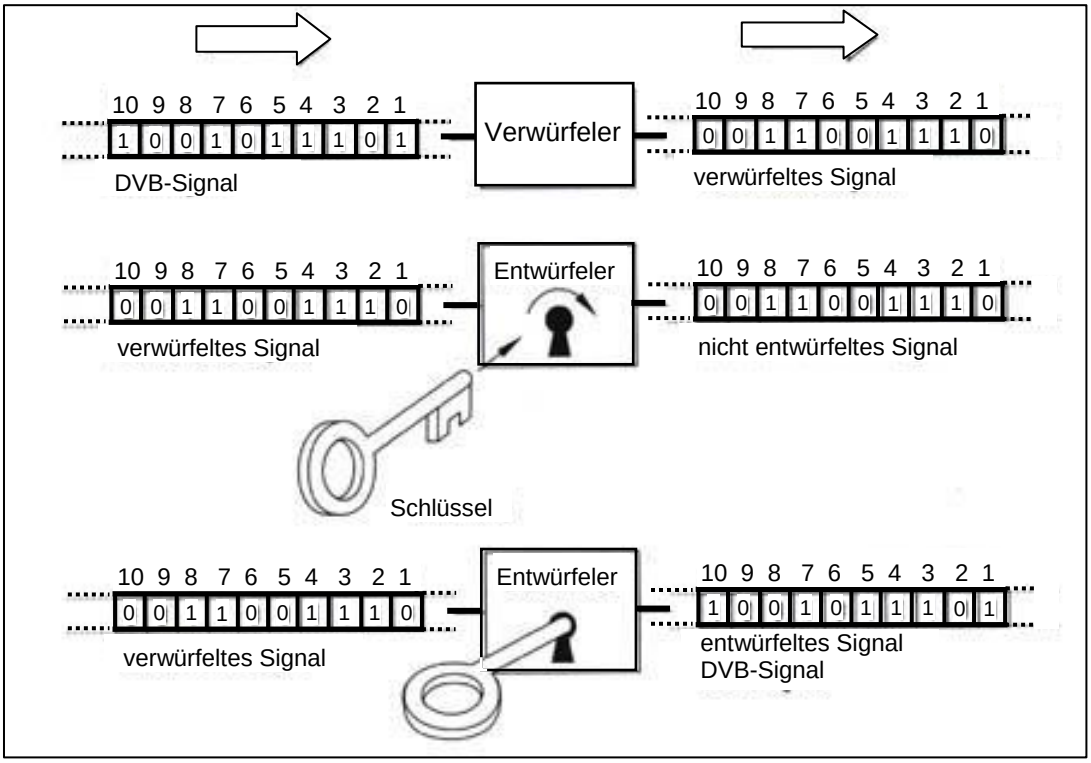
99 o.V., o.J.(29)

100 Schlomski, o.J.

Technisch präziser läuft dies folgendermaßen ab: Damit der Receiver eines berechtigten Pay-TV-Kunden das Programm entschlüsseln kann, werden die notwendigen Steuerinformationen zur Identifizierung des CA-Systems in Form der Conditional-Access-Tabelle (CAT) mit dem Digitalsignal des DVB-Systems ausgestrahlt. In der Tabelle ist für jedes Verschlüsselungssystem eine bestimmte CAS-ID (Conditional Access System - Identifier Data) verzeichnet. Die Verschlüsselung der Video- und Audiodaten selbst erfolgt unabhängig vom CA-System durch den Common Scrambling Algorithm (CSA), der in der Hardware des Receivers integriert ist. Um das Signal zu entschlüsseln, muß der Algorithmus spezielle Control Words (CW) erkennen, die das CA-System des Pay-TV-Anbieters generiert und in Form von Entitlement Control Messages (ECM) im Datenstrom ebenfalls verschlüsselt mitüberträgt. Im Receiver des Kunden wird der gesamte Datenstrom an das Common Interface geleitet. Das angeschlossene CA-Modul filtert die ECMs anhand der Informationen der Program Map Tabelle (PMT) heraus und errechnet mit Hilfe des Schlüssels, der auf der Smartcard bzw. auf dem fest integrierten Chip gespeichert ist, das Control Word. Der Schlüssel kann durch spezielle Datenpakete, sogenannte Entitlement Management Messages (EMM), von Zeit zu Zeit geändert oder mit Sonderberechtigungen, z.B. für den zeitlich limitierten Zugang zu Pay-per-view-Angeboten, ausgestattet werden. Die Identifikationsdaten der EMMs sind ebenfalls in der CA-Tabelle verzeichnet.[101]

[101] Linow, 2004, S. 92

Abbildung 10:
Conditional Access (Funktionsprinzip)



Quelle: o.V., o.J.(27)

Bezüglich der Codierungsstandards wird zwischen den Verfahren Simulcrypt und Multicrypt differenziert. Simulcrypt ermöglicht die Ansteuerung verschiedener CA-Systeme durch das Transportsignal. Das selbe Programm kann also durch unterschiedliche CA-Systeme entschlüsselt werden. Das Multicryptverfahren ermöglicht auf Empfängerseite die Nutzung verschiedener Decodiersysteme mit Hilfe der CI-Schnittstelle. An die Schnittstelle können verschiedene CA-Module angeschlossen werden, so dass unterschiedliche Verschlüsselungen decodiert werden können.[102]

3.3.2. Anforderungen an das Verschlüsselungssystem

Die Verschlüsselungstechnik muss einer Reihe von Anforderungen genügen. Grundvoraussetzung ist die Kompatibilität mit dem jeweiligen Fernsehsignalsystem innerhalb des Ausstrahlungsgebietes. Für die Bundesrepublik Deutschland ist dies das PAL-System.[103] Das verschlüsselte Fernsehsignal muss problemlos auf allen vorgesehenen Distributionswegen übertragen werden können, im wesentlichen über Kabel und Satellit. Dabei ist auch sicherzustellen, dass das codierte Signal kompatibel zu sämtlichen Hausverteilanlagen und Endgeräten wie Satellitenreceiver, Fernsehempfänger und Videorecorder ist. Durch

[102] Posewang, 2004, S. 38

[103] Dinsel, 1991, S. 9

die Verschlüsselung darf es zu keinen wahrnehmbaren Beeinträchtigungen des entschlüsselten Bildes und Tons kommen.[104]

Erfolgskritisch für ein Pay-TV-Angebot ist der zuverlässige Empfang des Programms. Daher ist es unabdingbar, dass die Coder und Decoder reibungslos funktionieren.[105] Probleme mit der Technik, die dazu führen, dass der Fernsehgenus getrübt wird, verursachen Verärgerung bei der zahlenden Kundschaft[106]. Im schlechtesten Fall kündigen sie daraufhin ihr Abonnement, auch potentielle Kunden können durch solche Probleme abgeschreckt werden. Die Teilnehmerendgeräte sollten außerdem eine hohe Benutzerfreundlichkeit aufweisen, d.h. die Bedienbarkeit muss einfach und auch für technische Laien verständlich sein.[107] Die Decoder selbst sollten adressierbar sein, damit der Pay-TV-Anbieter jeden Teilnehmer zu- bzw. wieder abschalten kann: Zu Beginn des Vertrags wird der Decoder freigeschaltet, falls ein Teilnehmer nicht mehr bezahlt bzw. seinen Vertrag nicht verlängert, wird er wieder deaktiviert.[108]

Von wesentlicher Relevanz ist die Verschlüsselungssicherheit. Notwendig ist dabei eine ausreichend hohe Verschlüsselungstiefe[109]. Um das ausgestrahlte Sendesignal möglichst wirksam vor Hack-Attacken zu schützen, sollte der kryptographische Code so stark wie möglich sein, dass heißt, er sollte nur mit unverhältnismäßig viel Zeit und Aufwand illegal decodiert werden können.[110] Zusätzlich sollte in regelmäßigen Abständen ein Codewechsel vorgenommen werden.[111] Um permanent den bestmöglichen Schutz zu garantieren, erfolgen laufend Verbesserungen der Software, die mit immer leistungsfähigeren Digitaldecodern zusammenarbeiten. Beispielsweise versorgt der CAS-Produzent Irdeto Access seine Klientel alle zwölf bis achtzehn Monate mit einer neuen Smartcard-Generation auf neuestem technischen Stand.[112]

Neben der Stärke des Verschlüsselungsalgorithmusses ist für die Sicherheit des Verschlüsselungssystems jedoch auch noch ein zweiter Faktor von entscheidender Bedeutung: die Geheimhaltung des angewendeten Schlüssels.[113] Wird die Wirkungsweise des Schlüssels bekannt, verliert auch der komplizierteste Code seinen Effekt und wird dadurch wertlos. Darüber hinaus muss sicher-

---

[104] Haas, 1991, S. 35f.

[105] Lenhardt, 1991, S. 5

[106] Siehe Kapitel 3.3.6., Probleme mit der Verschlüsselungstechnik am Beispiel Premiere.

[107] Haas, 1991, S. 39f.

[108] Sewczyk, 1991, S. 27

[109] Die Verschlüsselungstiefe hängt zum einen von der Leistungsfähigkeit des Algorithmusses, zum anderen von der Länge des Schlüssels, mit der der Algorithmus arbeitet, ab. Siehe hierzu: o.V., o.J.(28).

[110] Vgl. o.V., 1999, S. 2f.

[111] Posewang, 2004, S. 38

[112] ebenda, S. 38f.

[113] Vgl. o.V., 1999, S. 2f.

gestellt werden, dass die Zugangsdaten durch die autorisierten Nutzer, also die Pay-TV-Kunden, nicht weitergegeben werden.

Trotz aller Fortschritte und Verbesserungen der Verschlüsselungen existiert kein Datensicherheitssystem, welches absolut sicher ist.[114] Auch der gegenwärtig leistungsfähigste kryptographische Code wird wahrscheinlich mit Hilfe zukünftiger Technologie bald geknackt werden.[115] Sofern diese Bedrohung nicht mehr mit einfachen Codewechseln wirksam bekämpfbar ist, kann eine Umstellung des gesamten Verschlüsselungssystems notwendig werden. Diese sollte so einfach und kostengünstig wie möglich durchzuführen sein. Es bietet sich dabei an, diese Umstellung auf Empfängerseite nur durch den Austausch einer Chipkarte durchzuführen.[116] Die Decodierung sollte daher zweistufig mit Hilfe einer Decoderbox und einer intelligenten Chipkarte, der Smartcard, erfolgen.[117] Durch die Systemumstellung werden bis dahin genutzte Piratengeräte und -karten unbrauchbar gemacht.[118] Da zumindest auf lange Sicht mit dem Hack des genutzten Verschlüsselungssystems gerechnet werden muss, sollte diese Option bereits bei der Auswahl des Systems eingeplant werden.

Ebenfalls eine wichtige Rolle für die Auswahl eines Verschlüsselungssystems spielt der Kostenaspekt. Dabei sind die Kosten der Anschaffung, bestehend aus dem Kaufpreis und den zusätzlich entstehenden Transaktionskosten in Form von Informations-, Aushandlungs- und Durchsetzungskosten[119], wie auch die anfallenden laufenden Kosten des Betriebs relevant. Das genutzte System sollte daher einen möglichst niedrigen Beschaffungspreis haben und gleichzeitig kostengünstig im Unterhalt sein.[120]

3.3.3. Wichtige aktuelle Verschlüsselungssysteme

Gegenwärtig gibt es eine Reihe verschiedener Verschlüsselungssysteme.[121] Das Verschlüsselungssystem „Videoguard“, entwickelt von Rupert Murdochs Firma NDS,[122] wird für die britische Sky-Digital-Plattform und den italienischen Ableger Sky Italia sowie von TV Polonia verwendet. Videoguard hat bisher offenbar allen Angriffsversuchen widerstanden. Wie für Videoguard ist auch für das System „PowerVu“ kein Common-Interface-Modul nötig, es kommt daher ohne Smartcard aus. Der Receiver muß vom Programmanbieter autorisiert und freigeschaltet werden, Manipulationen gelten dabei als ausgeschlossen. In Mitteleuropa wird PowerVu nur noch von AFRTS (Armed Forces Radio and Televi-

---

[114] Zimmermann, 1999, S. 57

[115] Vgl. o.V., 1999, S. 3.

[116] Hunsel, 1991, S. 56

[117] Haas, 1991, S. 36

[118] Vgl. Hunsel, 1991, S. 56.

[119] Blum, 1994, S. 451

[120] Vgl. Lenhardt, 1991, S. 7.

[121] Hagedorn, 2004b, S. 20

[122] o.V., o.J.(29)

sion Service[123]) verwendet.[124] Das erste „Irdeto"-System wird von der niederländischen Nethold-Gruppe vermarktet[125] und ist wie der Ableger „Betacrypt" geknackt. Es wird lediglich noch in den Niederlanden von Canal Digitaal verwendet. Das neue „Irdeto 2" gilt bisher als piratensicher.[126] Die Weiterentwicklung von „Nagravision", „Nagravision 2/Aladin" der Schweizer Kudelski-Group[127], gilt zur Zeit ebenfalls als sicher. Es wird u.a. von Premiere, Kabel Digital und Digital+ verwendet.[128] Die von der französischen Firma „Société Européenne de Controle d' Access"[129] stammende „Seca/Mediaguard"-Verschlüsselung ist sowohl in der ersten als auch in der aktuellen zweiten Version geknackt worden. Dennoch nutzt das italienische DVB-T-Paket „D Free" das System Mediaguard 1. Philips entwickelte „Cryptoworks", welches z.B. von Xtra Music, UPC Direkt, DigiTurk, BFBS und iTV Partner eingesetzt wird. Für einige dieser Anbieter sind Codes zur illegalen Entschlüsselung bekannt. „Viaccess", eine Entwicklung der France Telecom[130], wird in der aktuellen zweiten Version vor allem in Frankreich, der Schweiz und in Skandinavien eingesetzt. Viaccess 1 ist geknackt. Die Verschlüsselungstechnik von „Conax" kommt bei Canal Digital in Skandinavien zum Einsatz. Trotz immer kürzerer Abstände bei den Keywechseln konnte dieses System der norwegischen Firma Telenor[131] nicht erfolgreich vor Piraten schützen.[132] Auch die deutsche Pay-TV-Plattform „kabelVision" verschlüsselt ihre Pay-TV-Programme und Pay-per-view-Dienste in Conax.[133] Eine Übersicht über Verschlüsselungssysteme zeigt die folgende Abbildung.

---

[123] o.V., o.J.(2)
[124] Hagedorn, 2004b, S. 20
[125] o.V., o.J.(29)
[126] Hagedorn, 2004b, S. 20
[127] o.V., o.J.(29)
[128] Hagedorn, 2004b, S. 20
[129] Mitiu, 2004
[130] o.V., o.J.(29)
[131] ebenda
[132] Hagedorn, 2004b, S. 20
[133] o.V., 2005(2)

Abbildung 11:
Übersicht von aktuellen Verschlüsselungssystemen und deren Verwendern

Verschlüsselungssysteme

Anbieter	CA-System	Deutschland	Europa
Nagra (1)	Nagravision	Premiere, Kabel Deutschland, VisAvision	ORF, Xtend (Eutelsat), Telewest, NTL (GB), Polsat, Antenna Hungaria
Motorola	Mediacipher		Ono (Spanien), NDS, AsterCity (Polen)
Scientific Atlanta.	PowerKey	ish	NTL (GB), CAI Westland (NL)
Mediaguard (1)			Canal+, Canal Satellite, BBC
NDS	Videoguard		BSkyB, NTL, Telewest, Sky Italia
Viaccess	Viaccess		TPS (F), Canal+ Horizon (F), NTV+ (Rus), France Telecom Cable, UPC (F), Casema (NL), ViaSat
Irdeto Access	M-Crypt Irdeto PIsys		Apollo 13 (I), Zee TV (GB), Canal+ (NL), Telepiu, Stream (I, jetzt NDS) weitere europäische Programme wie Playboy TV (GB)
Philips	Cryptoworks	Primacom, DFA, ORF (2) Deutsche Telekom (Business TV)	Eurosport, CLT-RTL, Viacom, MTV, UPC Direct, Viva Polska, XtraMusic (Radio)
Conax	Conax	ewt, Bosch Breitbandkabel, Tele Columbus, Martens, Komro, Vikom, VisavisionDeutsche Telekom	Digiteene (NL), Canal Digital in Skandinavien und weitere

rfe

Quelle: Posewang, 2004, S. 39

3.3.4. Kosten des Verschlüsselungssystems

Von entscheidender wirtschaftlicher Bedeutung ist der Preis des gesamten Verschlüsselungssystems.[134] Dabei gilt allgemein, dass eine erhöhte Verschlüsselungssicherheit mit einem erhöhten Kostenaufwand verbunden ist.[135]

Während in den USA allein der jeweilige Kabelnetzbetreiber bei gleichzeitiger Kostenübernahme festlegt, welche Verschlüsselung eingesetzt wird, obliegen in Europa Auswahl, Anschaffung und Betrieb des Codiersystems in der Regel den Pay-TV-Anbietern.[136] Auch die in Deutschland seit kurzer Zeit neben Premiere als Pay-TV-Anbieter auftretenden Kabelnetzbetreiber legen selbst ihre Verschlüsselungstechnik fest. Der DVB-Standard ermöglicht dabei eine freie Wahl des Codiersystems.[137]

Die Auswahl eines bestimmten CA-Systems hängt zum einen von den Programmen und Diensten (Pay-per-channel, pay-per-view etc.) ab, die angeboten werden sollen, zum anderen von den Kosten und Preisen, zu denen das Sy-

[134] Haas, 1991, S. 39f.
[135] Dinsel, 1991, S. 18.
[136] Vgl. Haas, 1991, S. 34.
[137] Linow, 2004, S. 92

stem erworben werden kann.[138] Das angewendete Verschlüsselungssystem kann entweder eine Eigenentwicklung[139] sein, oder es wird auf ein bereits vorhandenes Verfahren eines anderen Anbieters gegen Zahlung eines Kaufpreises zurückgegriffen.[140] Bekannte Anbieter von Conditional-Access-Systemen sind, wie bereits erwähnt, Nagravision, Mediaguard/Seca, Conax, Irdeto oder Cryptoworks. Oft kommt auch ein System zum Einsatz, welches der Sender zusammen mit einem Verschlüsselungsspezialisten in Gemeinschaftsarbeit entwickelt hat.[141] Auch der Einsatz mehrerer Verschlüsselungssysteme gleichzeitig ist möglich (als Simulcrypt bezeichnet).[142] Bei der Wahl des Verschlüsselungssystems muss der Sender außerdem entscheiden, ob er bei der Decodiertechnik, die für die Anwendung der CA-Systeme notwendig ist, auf einen oder mehrere Lieferanten zurückgreifen möchte. Hierbei steht einer erhöhten Flexibilität, schnelleren Liefermöglichkeiten sowie einer geringeren Abhängigkeit von Lieferanten bei mehreren Zulieferern ein erhöhter Koordinationsaufwand gegenüber.[143]

Bei Fremdbezug des Systems entstehen dem Pay-TV-Anbieter zunächst Transaktionskosten in Form von Such- und Anbahnungskosten bei der Auswahl des Systems und der Lieferanten, Kosten während der Vertragsverhandlungen bis zum Vertragsabschluß, Kosten für die Kontrolle der Vertragseinhaltung und Kosten für eventuell erforderliche Vertragskorrekturen. Bei Eigenentwicklung des Systems fallen Kosten für die Entwicklung an, insbesondere bestehend aus den Arbeitsstunden der an dem Projekt beteiligten Mitarbeiter und den Kosten für die zur Entwicklung erforderliche technische Ausstattung. Wird auf einen Fremdhersteller zurückgegriffen, erfolgt die Entwicklung des Codiersystems sinnvoller Weise in Zusammenarbeit mit dem Pay-TV-Sender. Dies bedeutet, dass Mitarbeiter des Senders an der Entwicklung und Implementierung beteiligt sind und hierfür entsprechend Zeit aufwenden müssen. Es muss abgewogen werden, wie viele Mannstunden investiert werden sollen, um die gewünschte Qualität des Systems zu erreichen. Diese Kosten addieren sich zu dem Kaufpreis des Systems. In jedem Fall entstehen Kosten für die Evaluierung des Systems und der Software, Investitionskosten für die Encoder und die Datenübertragungstechnik, Investitionskosten für die Decoder, Herstellungskosten für die Chipkarte, Kosten für die Erstausstattung der Kunden mit Decoder und Chipkarte und Kosten für die Lagerhaltung der Decoderboxen und Smartcards inklusive Verzinsung bis zur Auslieferung.[144] Die technische Ausstattung wird über die

---

[138] Posewang, 2004, S. 39

[139] Z.B. betreibt Kabel Deutschland (KDG) eine eigene digitale Plattform für die Ver- und Entschlüsselung, bestehend aus einem Verschlüsselungssystem, einem Decoder und einer Smart Card. Siehe hierzu z.B. o.V., 2004(7).

[140] Michaelsen, 1996, S. 76

[141] Z.B. verwendet Premiere eine Version von Nagravision, die von Kudelski gemeinsam mit Premiere entwickelt wurde. Vgl. hierzu: Hofmeir, Herres, 2003, S. 7.

[142] Linow, 2004, S. 92

[143] Michaelsen, 1996. S. 38f.

[144] Haas, 1991, S. 40

Nutzungsdauer abgeschrieben, da diese im Laufe der Zeit veraltet bzw. durch Piraterie-Angriffe unwirksam wird und daher nach einer Weile durch neue Technologie ersetzt werden muss.

Neben diesen Anschaffungskosten entstehen Kosten für den laufenden Betrieb des Verschlüsselungssystems.[145] Hierzu gehören die Erfassung der Kundendaten, Kundenservice in Form einer Kontaktmöglichkeit und eines Reparatur- und Austauschservices der Smartcards und Decoderboxen, sofern dies nicht von einem externen Zulieferer übernommen wird, sowie Unterhalts- und Wartungskosten der Verschlüsselungstechnik einschließlich regelmäßig vorzunehmender Codeänderungen und System-Updates.

Die Bereitstellung der Entschlüsselungstechnik beim Zuschauer kann durch das Verleihen, Vermieten oder Verkaufen der Decoder-Boxen erfolgen. Das Vermieten und in noch höherem Umfang das Verleihen der Decoder bedeuten für den Pay-TV-Anbieter einen erheblichen finanziellen Aufwand. Jedoch tragen diese Varianten erheblich zur Kundengewinnung bei, da die Kunden auf diese Weise eine relativ hohe Anfangsinvestition vermeiden können und damit der Widerstand gegen die Nutzung des zahlungspflichtigen Angebots sinkt.[146] Besonders in der Anfangszeit des deutschen Pay-TV war der Aufwand für die Entwicklung eines Pay-TV-Decoders enorm hoch, so dass es nur bedingt möglich war, die Kosten und den Aufwand auf der Senderseite zu bündeln, um den Empfangsdecoder möglichst billig zu halten.[147] Premiere investierte beispielsweise in die Entwicklung der ersten Decoder mehrere Hundert Millionen DM.[148] Gegenwärtig nutzt Premiere die Preisgestaltung der Receiver, um einen Anreiz für die Bestellung eines teuren Programmpakets zu geben und gleichzeitig einen Receiver zu kaufen statt zu mieten: je teurer das georderte Programm, desto billiger ist der Receiver. Bei Bestellung des teuersten Programmpakets erhält der Kunde einen stark subventionierten Decoder für 1,- Euro[149]. Der Verlust, der bei Abgabe des Receivers unter dem Einkaufspreis entsteht, muss anschließend auf anderem Wege, beispielsweise durch die Abonnementgebühren, wieder erwirtschaftet werden.

Die Smartcard wird den Kunden häufig unentgeltlich bereitgestellt. Dabei kann der Lieferant des Verschlüsselungssystems der Eigentümer der Karte bleiben, so dass dem Pay-TV-Anbieter hierfür keine zusätzlichen Einkaufskosten entstehen, falls er sie unentgeltlich zur Verfügung gestellt bekommt, oder ein Mietzins an den Lieferanten geleistet werden muss, falls die Karten gemietet werden. Im Fall von Premiere bleibt die Smartcard z.B. das Eigentum von Nagravision.[150]

---

[145] Vgl. ebenda, S. 40.

[146] Michaelsen, 1996, S. 76

[147] Dinsel, 1991, S. 9

[148] Hunsel, 1991, S. 52

[149] Stand: Dezember 2004

[150] o.V., o.J.(5)

Der Versand der Decoder und der Smartcards ist mit Auslieferungskosten und Portogebühren verbunden. Oft werden diese Kosten in Form von Versandkostenpauschalen und Nachnahmegebühren an die Kunden weitergegeben. Einige Anbieter berechnen den Kunden zusätzlich Bereitstellungs- oder Aktivierungsgebühren, um auch die durch den organisatorischen Aufwand entstehenden Kosten an den Neukunden weiterzureichen.

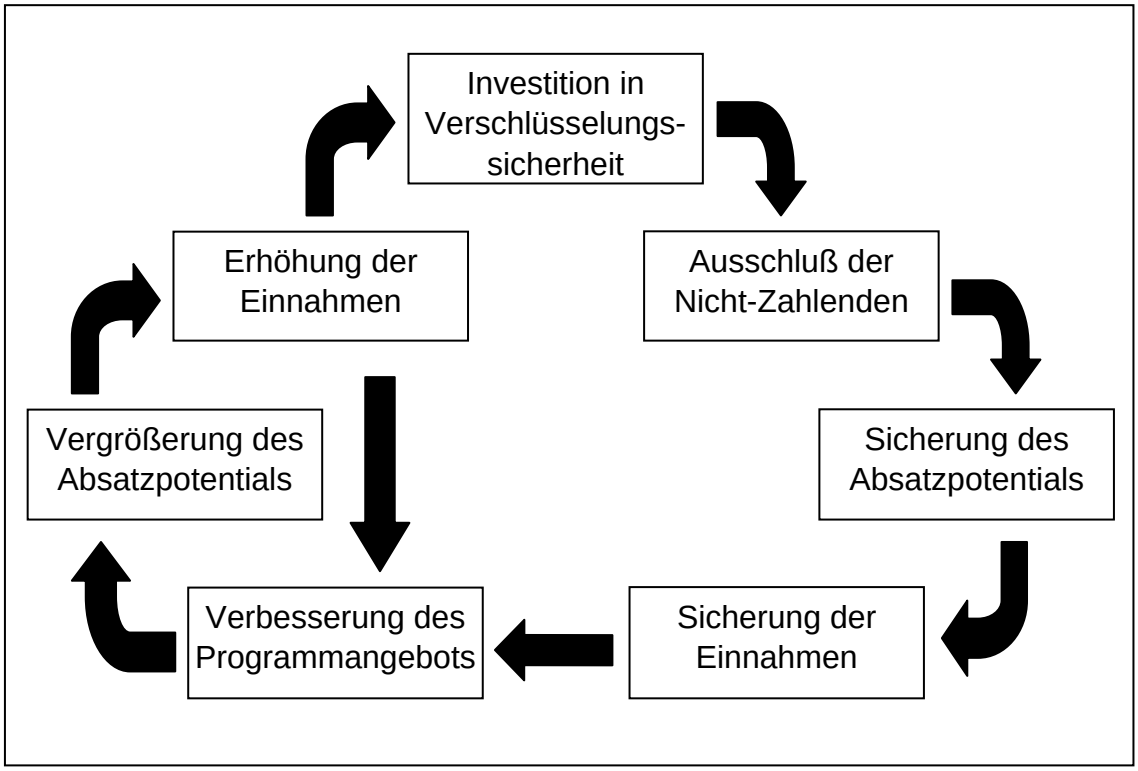
3.3.5. Nutzen der Verschlüsselung

Das Verschlüsselungssystem ist für einen Pay-TV-Anbieter unerlässlich. Ohne Verschlüsselung wäre das Programm frei empfangbar und es bestünde für die Zuschauer kein Anreiz, Gebühren an die Sender abzuführen. Die Investition in das Verschlüsselungssystem dient der Sicherung der Einnahmen, in dem nur denjenigen Zuschauern die notwendige Entschlüsselungstechnik bereitgestellt wird, die sich vertraglich zur Zahlung der anfallenden Gebühren verpflichten und diese auch zuverlässig leisten.

Leistungsfähige Verschlüsselungstechnologien können Piraterie technisch schwierig und kommerziell unattraktiv machen.[151] Die Verwendung einer Verschlüsselung, die Nicht-Zahlende zuverlässig ausschließt, trägt dazu bei, das Absatzpotential zu bewahren. Solange die Zuschauer keine Möglichkeit haben, die Verschlüsselung auf kostengünstige Weise zu umgehen, werden sie registrierte Kunden bleiben bzw. legale Abonnenten werden, vorausgesetzt, die Kunden sind mit dem angebotenen Programm und dem Preis zufrieden. Die Verschlüsselung kann außerdem dazu beitragen, das Absatzpotential zu vergrößern: Da dem Sender keine Einnahmen entgehen, kann er die eingenommenen Gelder in die Verbesserung seines Programmangebots investieren, z.B. durch den Einkauf weiterer und eventuell teurer Programminhalte. Das verbesserte Programm kann aufgrund der höheren Attraktivität einen größeren potentiellen Kundenkreis ansprechen, dessen Zahlungsbereitschaft erhöhen und damit das Absatzpotential erweitern. Werden tatsächlich mehr zahlende Kunden gewonnen, können mehr Einnahmen generiert werden, die neben Investitionen in die Verschlüsselungssicherheit zur Bewahrung des Absatzpotentials und zur Sicherung der Einnahmen wiederum in eine Verbesserung des Programmangebots zur Erweiterung des potentiellen Kundenkreises investiert werden können (siehe Abbildung 12). Auch werden die Rechteinhaber gerne ihre Filmwerke bereitstellen, da sie sich darauf verlassen können, dass die Ausstrahlung tatsächlich nur den vereinbarten Zuschauerkreis erreicht. Dies ermöglicht dem Sender für sein Programm eine hohe Auswahlmöglichkeit und damit die Erzielung der gewünschten Programmqualität.

[151] Lievaart, 2001, S.1

Abbildung 12:
Nutzen der Verschlüsselung



Quelle: Eigene Darstellung

Zusätzlich entstehen dem Sender Einnahmen aus dem Verkauf oder der Vermietung von Decoderboxen, die in Gewinnen resultieren können, sofern die Verkaufserlöse bzw. Mieteinnahmen den Einkaufspreis der Decoder zzgl. aller übrigen Beschaffungskosten übertreffen. Werden dem Pay-TV-Kunden Receiver und/oder Smartcard gegen Hinterlegung einer nicht verzinsten Kaution bereitgestellt, kann der Pay-TV-Anbieter die aus den Kautionsbeträgen entstehende Zinsgewinne abschöpfen und als zusätzliche Einnahmen verbuchen. Ebenso verlangen einige Sender von einem Neukunden einmalige Zahlungen in Form von Aktivierungs- oder Freischaltungsgebühren, die, sofern sie nicht nur kostendeckend sind, ebenfalls zum Gewinn beitragen können.

Wird auf eine Verschlüsselung verzichtet oder ein geknacktes Verschlüsselungssystem verwendet, sind Schwarzseher unvermeidlich. Potentielle Kunden werden auf eine eventuell günstigere Schwarzseh-Option aufmerksam und ziehen diese einem regulären Abonnement vor, bisherige Abonnenten kündigen und konsumieren die Sendungen zukünftig ohne Abo-Gebühren. Auf diese Wiese gehen einem Pay-TV-Anbieter Absatzpotential und tatsächliche Kunden verloren, in Folge sinken auch die Einnahmen des Senders. Kritisch anzumerken ist hier jedoch, dass ein Ausschluss von Schwarzsehern nicht zwangsläufig mit einer Erhöhung der Abonnentenzahl verbunden sein muss. Sofern die Zahlungsbereitschaft der Schwarzseher geringer ist als der Preis eines regulären Abonnements, werden sie auch dann nicht zu zahlenden Kunden werden, wenn ein illegaler Empfang nicht mehr möglich ist. Des weiteren ist davon auszuge-

hen, dass früher oder später jede technische Schutzvorkehrung durch Pay-TV-Piraten umgangen werden wird und ein dauerhafter Ausschluss sämtlicher Schwarzseher zum gegenwärtigen Zeitpunkt nicht wahrscheinlich erscheint.

3.3.6. Probleme mit der Verschlüsselungstechnik: Beispiel Premiere

Um die bisherigen Schwarzseher von weiterer illegaler Nutzung auszuschließen, wurde im September 2003 das Verschlüsselungssystem bei Premiere gewechselt. Anstelle des geknackten Betacrypt-Systems kommt seitdem eine speziell entwickelte Version von Nagravision zum Einsatz[152], die gegenwärtig Schutz vor allen zur Zeit bekannten Angriffsarten bietet.[153] Bei dieser Technik erfolgte anfangs eine Änderung des Dekodierungsschlüssels alle 80 Sekunden. Nach wenigen Wochen stellte sich heraus, dass diese Zeitspanne zu lang war und eine Sicherheitslücke darstellte, die von Hackern bereits ausgenutzt wurde. Als Reaktion darauf wurde der Änderungszyklus des Schlüssels auf unter 10 Sekunden verkürzt. Dies führte jedoch zu technischen Problemen bei den legalen Empfängern, die sich über Ruckler und Bildaussetzer beschwerten. In anderen Fällen empfingen die Nutzer statt eines Premiere-Programms nur den Hinweis, ihre Karte sei nicht freigeschaltet.[154] Diese Beeinträchtigungen bestanden für die Nutzer wochenlang. Laut Premiere war dies auf die Überlagerung von drei verschiedenen technischen Problemen zurückzuführen: Neben dem Schlüsseländerungsproblem existierte ein defekter Chip in der Sendetechnik, außerdem entstanden bei einigen Digitalreceivern Asynchronitäten zwischen Bild und Ton.[155]

Zweifellos ist es ein schwerwiegendes Problem, wenn Kunden eine bereits bezahlte Leistung, nämlich die ausgestrahlten Fernsehprogramme, nicht oder nur in unbefriedigender Qualität empfangen können. Neben einer Imageschädigung des Unternehmens kann die Verärgerung der Kunden zu Regreßansprüchen von Kundenseite in Form von Erstattungen der gezahlten Beiträge führen oder gar Kündigungen des Abonnements nach sich ziehen. Durch die Publikmachung solcher Nachrichten und die negativen Erfahrungsberichte von Abonnenten im Freundeskreis, Internetforen u.ä. werden auch potentielle Pay-TV-Kunden von einem Abonnement Abstand nehmen. Maßnahmen der Piraterie-bekämpfung können also dazu führen, dass vorhandene Kunden verloren gehen bzw. potentielle Kunden abgeschreckt werden, mit entsprechenden Einnahmeeinbußen als Folge. Selbst wenn der Pay-TV-Anbieter bei derartigen technischen Störungen Entschädigungen vom Lieferanten der Verschlüsselungstechnik fordern könnte, würde die Geltendmachung der Forderungen wiederum zu Aufwand und Kosten führen. Der erlittene Imageschaden bleibt jedoch auch dann zunächst bestehen.

---

[152] Vgl. Hofmeir, Herres, 2003, S. 7.

[153] Hankmann, Sprotte, 2004e

[154] Porteck, 2004a

[155] ders., 2004b

3.3.7. Kosten-Nutzen-Abwägung der Verschlüsselung

Eine solide Verschlüsselungstechnik ist zur Abwehr illegaler Nutzer unbedingt erforderlich. Dennoch muss der Einsatz des Verschlüsselungssystems dem Prinzip der Wirtschaftlichkeit Genüge tun und ein angemessenes Kosten-Nutzen-Verhältnis aufweisen. Dabei muss der Nutzen, der durch die Verwendung des Verschlüsselungssystems entsteht, alle damit zusammenhängenden Kosten überwiegen, ansonsten ist der Einsatz der Verschlüsselung nicht rational.

Der Nutzen einer Verschlüsselung besteht, wie zuvor angeführt, im wesentlichen aus der Bewahrung der Einnahmeströme durch die Vermeidung von Abonnentenverlusten wegen günstigerer Schwarzseh-Alternativen und der Gewinnung neuer Abonnenten, die aufgrund der gegebenen Attraktivität des Programms in den Genuss des Pay-TV kommen möchten und zahlende Abonnenten werden. Es ist also zu schätzen, wie viele Zuschauer allein wegen mangelnder Schwarzseh-Möglichkeiten Abonnenten sind und welche Gebühren-Einnahmen dadurch entstehen. Zusätzlich muß beziffert werden, welche Einnahmen aus der Absatzpotentialerweiterung generiert werden können, also wie viele zahlende Abonnenten aufgrund der Qualitätsverbesserung des Programms, die durch die gesicherten Einnahmeströme realisiert werden kann, hinzukommen. Hinzu gerechnet werden die Einnahmen aus den Zinsgewinnen der Kautionszahlungen für Smartcards[156] sowie für verliehene oder vermietete Decoder, die einmaligen Einnahmen aus dem Verkauf bzw. die regelmäßigen Einnahmen aus der Vermietung eines Decoders und Einmalzahlungen in Form von Aktivierungsgebühren bei Vertragsabschluß. Letztere Beträge resultieren aus den Einnahmen von allen Abonnenten, da ebenfalls die ehrlichen Kunden, die auch ohne Verschlüsselung oder bei Existenz von Schwarzseh-Möglichkeiten die Gebühren ordnungsgemäß an den Pay-TV-Anbieter zahlen würden, Zahlungen für Kautionen, Decoder und Aktivierung leisten müssen.

In einer Formel ausgedrückt, setzt sich der Nutzen folgendermaßen zusammen:

$$N_V = E_{SKA} + E_{EKA} + E_{KS} + E_{KD} + E_{DV} + E_{DM} + E_A ,$$

mit:

N_V: Nutzen, der aus der Anwendung des Verschlüsselungssystems resultiert

E_{SKA}: Einnahmen durch Abonnementgebühren von Kunden, die nur aufgrund mangelnder Schwarzseh-Optionen zahlende Abonnenten sind (Sicherung des Kundenbestands und Absatzpotentials durch Verschlüsselung)

E_{EKA}: Einnahmen durch Abonnementgebühren aufgrund der durch die Verschlüsselung ermöglichten Erweiterung des Absatzpotentials und Kundenbestands

E_{KS}: Einnahmen durch Zinserträge aus den Smartcard-Kautionsbeträgen

E_{KD}: Einnahmen durch Zinserträge aus den Decoder-Kautionsbeträgen

---

[156] Beispielsweise verlangt „Kabelcom Rheinhessen“ eine Kaution für die Smartcard in Höhe von 15,- Euro. Siehe hierzu: o.V., o.J.(24).

E_{DV}: Einnahmen aus dem Verkauf von Decodern

E_{DM}: Einnahmen aus der Vermietung von Decodern

E_A: Einnahmen aus Aktivierungs- oder Freischaltgebühren oder ähnlichen Einmalzahlungen.

Die Betrachtung der Einnahmeströme erfolgt dabei über den gesamten Zeitraum, in dem das Verschlüsselungssystem verwendet wird. Sofern der Pay-TV-Anbieter für einzelne der oben angeführten Posten keine Entgelte verlangt, entfallen diese in den Gleichungen.

Für die Berechnung der Einnahmen, die ausschließlich durch den Ausschluss der Schwarzseher entstehen, wird der durchschnittliche Umsatz pro Abonnent (ARPU – Average Revenue Per User) pro Zeiteinheit (z.B. pro Jahr) mit der Anzahl dieser Abonnenten multipliziert. Als Anzahl der Abonnenten wird deren Mittelwert über den Betrachtungszeitraum herangezogen, da permanent neue Abonnenten hinzukommen bzw. Verträge gekündigt werden können. Auch kann dadurch ein eventueller Abonnentenrückgang berücksichtigt werden, sollte das System während der Nutzungsdauer geknackt werden. Die Einnahmen aus den Abonnementgebühren der ehrlichen Zuschauer, die auch ohne Verschlüsselung für das Angebot zahlen würden, werden in dieser Gleichung nicht berücksichtigt, da hier lediglich der zusätzliche Nutzen in Form der aus den Verschlüsselungsmaßnahmen resultierenden Einnahmen betrachtet wird.

Daraus ergibt sich:

$E_{SKA} = ARPU/t * x_{SKA} * T$,

mit

ARPU/t: Durchschnittlicher Umsatz pro Abonnent pro Zeiteinheit

x_{SKA}: durchschnittliche Anzahl der Abonnenten innerhalb der Zeitperiode T, die nur aufgrund wirksamer Verschlüsselung zahlende Kunden sind

t:: Zeiteinheit

T: $\sum$ t als gesamter Betrachtungszeitraum, in dem das Verschlüsselungssystem verwendet wird.

Ähnlich berechnen sich die Einnahmen aus den zusätzlich gewonnenen Abonnenten aufgrund der hohen Programmqualität, die mit Hilfe der gesicherten Einnahmen realisiert werden kann. Es werden die durchschnittlichen Einnahmen dieser Abonnenten innerhalb des betrachteten Zeitraums ermittelt:

$E_{EKA} = ARPU/t * x_{EKA} * T$,

mit

x_{EKA}: durchschnittliche Anzahl der Abonnenten, die im Zuge der Kundenbestands- und Absatzpotentialerweiterung aufgrund der Programmqualitätsverbesserung zu zahlenden Kunden werden.

Die Zinsgewinne errechnen sich aus der Kautionshöhe, dem Zinssatz und der Anzahl der Abonnenten, die die Kaution leisten. Wird für die Smartcard eine

Kaution verlangt, sind hiervon alle Abonnenten betroffen, da jeder Abonnent die Smartcard für den Zugang benötigt. Kautionszahlungen für Decoder werden von denjenigen Kunden geleistet, die vom Pay-TV-Anbieter einen Leih- oder Mietdecoder in Anspruch nehmen. Für den Zinssatz pro Zeiteinheit (z.B. per annum) ist der Zinssatz der gewählten Anlageform der Kautionsbeträge anzusetzen. Dieser kann dabei je nach aktuellem Zinsniveau, Höhe des Betrags und Laufzeit der Anlage variieren. Die Gleichungen hierfür lauten:

$E_{KS} = Ka_S * i/t * x * T$ und

$E_{KD} = Ka_D * i/t * x_{DM} * T$,

mit

Ka_S: Kautionsbetrag pro Abonnent für die Smartcard

Ka_D: Kautionsbetrag pro Abonnent für einen geliehenen oder gemieteten Decoder

i: durchschnittlicher Zinssatz in Prozent innerhalb der Zeitperiode T

x: durchschnittliche Anzahl aller Abonnenten innerhalb der Zeitperiode T

x_{DM}: durchschnittliche Anzahl der Abonnenten innerhalb der Zeitperiode T, die den Decoder bei dem Pay-TV-Anbieter geliehen oder gemietet haben.

Die Einnahmen aus dem Verkauf der Decoder resultieren aus dem Preis eines Decoders und der Anzahl der verkauften Decoder innerhalb der Betrachtungsperiode.

$E_{DV} = p_D * D_K$,

mit

p_D: Verkaufspreis eines Decoders

D_K: Anzahl der verkauften Decoder innerhalb der Betrachtungsperiode.

Die Einnahmen aus der Vermietung der Decoder ergeben sich aus der Höhe der Mietrate pro Zeiteinheit (z.B. pro Monat), der Dauer des Betrachtungszeitraums und der durchschnittlichen Anzahl der vermieteten Decoder während dieses Zeitraums.

E_{DM}: $m_D/t * D_M * T$,

mit

m_D/t: Mietbetrag eines Mietdecoders pro Zeiteinheit

D_M: durchschnittliche Anzahl der vermieteten Decoder während des Betrachtungszeitraums.

Einmalzahlungen, die als Aktivierungsgebühren, Freischaltgebühren oder ähnliches bezeichnet werden, errechnen sich aus der Höhe der Gebühren und der Anzahl der Vertragsabschlüsse innerhalb des betrachteten Zeitraums.

$E_A = G * V$,

mit

G: Gebührenhöhe der Einmalzahlungen

V: Anzahl der Vertragsabschlüsse während des Betrachtungszeitraums.

Die zusätzlichen Kosten, die durch die Verschlüsselung während der Nutzungsdauer des Systems entstehen, setzen sich zusammen aus dem Kaufpreis des Systems bei externem Bezug zzgl. der damit verbundenen Transaktionskosten, Kosten für den eigenen Entwicklungsanteil (bei vollständiger Eigenentwicklung beträgt der Anteil 100%, so dass die Fremdbezugskosten entfallen), Kosten für die Implementierung des Systems, Kosten für die Technik, die den Kunden bereitgestellt wird, also Decoder und Smartcards (sofern die Smartcards nicht Eigentum des Verschlüsselungsanbieters bleiben[157]), Kosten für die Zertifizierung von Decodern und die Kosten für den laufenden Betrieb des Systems. Ebenfalls zu berücksichtigen sind die Finanzierungskosten des Systems.

$K_V = K_{KV} + K_{EV} + K_{IV} + K_{ZD} + K_{DS} + K_{BV} + K_F$,

mit:

K_V: Gesamtkosten des Verschlüsselungssystems

K_{KV}: Kosten des Kaufs eines Verschlüsselungssystems

K_{EV}: Kosten der Eigenentwicklung eines Verschlüsselungssystems

K_{IV}: Kosten für die Implementierung des Verschlüsselungssystems

K_{ZD}: Kosten für die Zertifizierung von Decodern

K_{DS}: durchschnittliche Kosten innerhalb der Zeitperiode T für die Beschaffung der Decoderboxen und Smartcards für die Abonnenten inkl. Lagerkosten und Verzinsung bis zur Auslieferung

K_{BV}: Kosten für den laufenden Betrieb des Verschlüsselungssystems während des Betrachtungszeitraums T,

K_F: Kosten für die Finanzierung des Verschlüsselungssystems.

Die Kosten für den Kauf eines Verschlüsselungssystems setzen sich zusammen aus dem Kaufpreis und den bereits erwähnten Transaktionskosten:

$K_{KV} = p_V + TAK$,

mit

p_V: Preis des Verschlüsselungssystems einschl. der notwendigen Technik

TAK: Transaktionskosten.

Die eigentlichen Kosten für die technischen Anlagen des Verschlüsselungssystems entstehen durch den Werteverzehr bzw. Wertverlust während der Nutzungszeit, der in Form von Abschreibungen bilanziell erfasst wird.[158] Da davon ausgegangen wird, dass das System zumindest solange genutzt wird, wie es nicht geknackt ist, und einem geknackten System ein Wert von Null zugeschrieben wird, da es seine Aufgabe nicht mehr ordentlich erfüllen kann, findet eine vollständige Abschreibung über die gesamte Nutzungszeit statt. Außerdem ist aufgrund der außerordentlich schnellen technologischen Entwicklung im Computerbereich von einem raschen Veralten der angeschafften Technik und

[157] In diesem Falle müßte evtl. eine Mietgebühr für die Smartcards entrichtet werden.

[158] Der eigentliche Anschaffungsvorgang ist buchhalterisch ein Aktivtausch und stellt damit keine Vermögensminderung dar.

einem damit einhergehenden hohen Wertverlust auszugehen. Daher wird in der Gleichung anstatt der Abschreibungsbeträge der Kaufpreis angesetzt, der der Summe aller Abschreibungsraten über die gesamte Nutzungszeit entspricht.

Die Kosten für die Eigenentwicklung der Verschlüsselung bestehen im wesentlichen aus den Investitionskosten für die benötigte Entwicklungs- und Systemtechnik (Hardware und Software) auf der Senderseite wie z.B. Encoder etc. und den Personalkosten, verursacht durch die eigenen Mitarbeiter, die an der Entwicklung des Systems beteiligt sind, z.B. Lohnkosten während der Entwicklungsdauer.

$K_{EV} = K_T + k_p/t * M * T$,

mit

K_T: Investitionskosten für die Technik auf der Seite des Pay-TV-Senders

k_p/t: Personalkosten pro Mitarbeiter und Zeiteinheit

t: Zeiteinheit, hier z.B. (Lohn) pro Stunde

M: Anzahl der an dem Projekt beschäftigten Mitarbeiter

T: Gesamtdauer der Entwicklung als $\sum$ t.

Auch hier werden anstatt der Abschreibungen auf die Technik die Investitionskosten angesetzt, da von einer vollständigen Abschreibung über die Nutzungsdauer ausgegangen wird.

Implementierungskosten bestehen ebenfalls hauptsächlich aus den Personalkosten der beteiligten Mitarbeiter des Pay-TV-Senders und des Verschlüsselungslieferanten:

$K_{IV} = k_p/t * M * T$.

Kosten für die Beschaffung von Decodern und Smartcards, falls diese vom Pay-TV-Sender vor der Weitergabe an den Kunden eingekauft werden, ergeben sich aus den Stückkosten multipliziert mit der jeweiligen Einkaufsmenge. Für die Decoder wird der Einkaufspreis angesetzt, da sie an die Kunden weiterverkauft werden und den Ausgaben nach kurzer Zeit Einnahmen gegenüberstehen. Erleiden die Decoder während der Lagerzeit einen Wertverfall, müssen hierfür entsprechende Abschreibungen getätigt werden, von denen hier abgesehen wird. Hinzu gerechnet werden müssen die Zins- und Lagerkosten, die aufgrund von Kapitalbindung und physischer Lagerung während der Lagerdauer bis zur Weitergabe an die Kunden entstehen. Hierfür wird der durchschnittliche Lagerbestand während der Betrachtungsperiode verwendet. Auch für die Smartcards wird der Einkaufspreis als Kosten angesetzt, sofern sie eingekauft werden. Da sie den Kunden unentgeltlich zur Verfügung gestellt werden, stellen sie für den Pay-TV-Anbieter während der gesamten Nutzungsdauer Kapitalbindung dar, daher muss das gebundene Kapital verzinst werden. Sollten die Karten vom Verschlüsselungslieferanten geliehen werden, entfallen diese Posten, werden sie für die Nutzungsdauer gemietet, muss der entsprechende Mietzins angesetzt werden.

K_{DS}: k_D*D + k_S*S_{KS} + m_S/t*S_{MS}*T + k_D * L_D * i/t * T + k_S*S_{DKS} *i/t * T + K_L ,

mit

k_D: durchschnittlicher Einkaufspreis der Decoder pro Stück innerhalb des Betrachtungszeitraums T

D: Anzahl der Decoder, die innerhalb der Zeitperiode T eingekauft werden

k_S: durchschnittlicher Einkaufspreis der Smartcards pro Stück innerhalb der Betrachtungsperiode T (im Falle des Smartcard-Kaufs)

S_{KS}: Anzahl der gekauften Smartcards innerhalb der Betrachtungsperiode T

m_S/t: Mietzins pro Smartcard pro Zeiteinheit (z.B. pro Monat) (im Falle der Anmietung von Smartcards)

S_{MS}: durchschnittlicher Miet-Smartcardbestand innerhalb der Betrachtungsperiode T

L_D: durchschnittlicher Lagerbestand an Decodern während der Betrachtungsperiode T

S_{DKS}: durchschnittlicher Bestand an gekauften Smartcards während der Betrachtungsperiode T

K_L: Kosten für die Lager einschließlich Lagerverwaltung etc. während der Betrachtungsperiode T.

Die Kosten für den laufenden Betrieb des Systems setzen sich im wesentlichen aus den Kosten für die technische Wartung wie Hard- und Software-Updates, Kosten für den Kundenservice wie Einspeisung und Pflege der Kundendaten, Kundenhotlines etc. und den Personalkosten der hierfür eingesetzten Mitarbeiter zusammen.

$K_{BV} = K_{TW} + K_{KS} + k_p/t * M * T$,

mit

K_{TW}: Kosten für die Wartung und den Unterhalt der Verschlüsselungstechnik während des Betrachtungszeitraums T

K_{KS}: Kosten für den Kundenservice während des Betrachtungszeitraums T.

Die Kosten für die Zertifizierung von Decodern K_{ZD} entstehen z.B. dem Sender Premiere, der alle Decoder zertifizieren muss, bevor sie für den Empfang von Premiere vertrieben und genutzt werden dürfen. Dies ist notwendig, um medienpolitischen und urheberrechtlichen Anforderungen zu entsprechen. Beispielsweise müssen die Decoder über einen sicheren und nicht abschaltbaren Jugendschutz verfügen. Außerdem muss Premiere den Hollywood-Studios eine kopiergeschützte Ausstrahlung über seine Pay-per-view-Kanäle zusichern, um die Spielfilme schon bald nach der Kino- und Videoauswertung zu einem entsprechend günstigen Preis zu erhalten. Für den Kopierschutz müssen die Decoder ein Störsignal an den Signalausgängen erzeugen.[159] Die während des Zertifizierungsprozesses entstehenden Kosten werden nur zum Teil den Deco-

[159] Hofmeir, 2005b, S. 22

derherstellern in Rechnung gestellt, den anderen Teil übernimmt Premiere, was somit eine weitere Kostenposition darstellt.[160]

Die Kosten der Finanzierung des Verschlüsselungssystems ergeben sich aus den Zinsbelastungen, die bei Fremdfinanzierung zu leisten sind. Werden Eigenmittel aufgewendet, entstehen Opportunitätskosten. Es muss ein Zinssatz angesetzt werden, mit dem das verwendete Eigenkapital bei alternativer Verwendung hätte verzinst werden können.

$K_F = FK * i_{FK}/t * T + EK * i_{EK} * T$,

mit

FK: durchschnittlicher Betrag des eingesetzten Fremdkapitals während der Betrachtungsperiode T

EK: durchschnittlicher Betrag des eingesetzten Eigenkapitals während der Betrachtungsperiode T

i_{FK}/t: durchschnittlicher Zinssatz des Fremdkapitals während der Betrachtungsperiode T pro Zeiteinheit

i_{EK}/t: durchschnittlicher Zinssatz pro Zeiteinheit während der Betrachtungsperiode T, mit dem das Eigenkapital bei alternativer Verwendung hätte verzinst werden können.

Damit der Einsatz einer Verschlüsselung eine rationale Entscheidung ist, muss der Nutzen, also die Summe aller Einnahmen, über die Nutzungszeit höher sein als die Summe aller Kosten, es muss gelten:

$N_V > K_V$.

Zur Illustration wird in einem vereinfachten Beispiel angenommen, ein Pay-TV-Anbieter vertreibe keine Decoder und verlange keine Kautionen oder Einmalgebühren. Seine zusätzlichen Einnahmen aus der Verwendung eines Verschlüsselungssystems resultieren demnach lediglich aus den Abonnementgebühren der verhinderten Schwarzseher E_{SKA}, die nur mangels Zugangsalternative zahlende Abonnenten sind, und der neu hinzugewonnenen Abonnenten E_{EKA} aufgrund der Attraktivität der ermöglichten Programmqualität. In Westeuropa betrug Ende 2003 der monatliche Durchschnittsumsatz pro Abonnent (ARPU) 21,70€,[161] dies entspricht 260,40€ im Jahr. Wird z.B. davon ausgegangen, daß 550.000 Zuschauer (dies sind etwa 20% des durchschnittlichen Premiere-Kundenbestands im Jahr 2003[162]) Abonnenten infolge der wirksamen Verschlüsselung sind, bewirkt die Ausschlussfunktion der Verschlüsselung einen jährlichen Umsatz von mehr als 143 Millionen Euro:

$E_{SKA}+_{EKA} = ARPU/t * x_{SKA+EKA} * T =$ 21,70€ * 550.000 *12 = 143.220.000,-€ .

---

[160] ders., 2005a

[161] Clover, 2004. Der ARPU-Wert wird für die Berechnungen beispielhaft verwendet, als Entscheidungsgrundlage muß jeder Sender seinen eigenen ARPU ermitteln. Für Premiere betrug dieser 2004 286,-€ im Jahr oder 23,83€ pro Monat, resultierend aus Aboverträgen, Pay-per-view und Werbeeinnahmen. Siehe hierzu: o.V., 2005(1).

[162] o.V., 2005(1)

Ist die Verschlüsselung also für die Dauer eines Jahres wirksam, dürfen die gesamten Kosten für die Verschlüsselung 143,22 Millionen Euro nicht überschreiten, um eine ökonomisch rationale Investition zu sein. Entsteht ein Einnahmeüberschuss, kann die Nutzung des Verschlüsselungssystems sogar zu einer Gewinnsteigerung des Unternehmens beitragen.

Ziel ist es also, zum einen so viel Einnahmen wie möglich zu generieren, zum anderen die Kosten so niedrig wie möglich zu halten. Hierzu muss insbesondere die Wirksamkeitsdauer und damit der Lebenszyklus des mit erheblichem Investitionsaufwand verbundenen Verschlüsselungssystems maximiert werden. Um dies zu erreichen, sollte von vornherein ein so hoher Sicherheitsstandard erreicht werden, dass er Hack-Bemühungen für Piraten finanziell unattraktiv macht. Gleichzeitig sollte das System auch über technische Fähigkeiten verfügen, mit denen wirksam, schnell und kostengünstig auf zukünftige unvermeidbare Piraten-Attacken reagiert werden kann, beispielsweise durch schnell und unkompliziert einspielbare Verschlüsselungs-Updates.[163]

Für die Ermittlung der Wirtschaftlichkeit ist die möglichst genaue Ermittlung der Einnahme- und Kostengrößen erforderlich. In der Praxis sind hiermit jedoch Schwierigkeiten verbunden. Die Dauer der Wirksamkeit eines Verschlüsselungssystems, also bis zu dem Zeitpunkt des Knackens durch Piraten, kann nicht prognostiziert werden. Beispielsweise wurde in der Anfangszeit von Premiere für die eingesetzte Verschlüsselung die Sicherheit vor Piraterie für einen Zeitraum von mindestens fünf bis sieben Jahren für notwendig erachtet, da ein früherer Decoderaustausch mit prohibitiv hohen Kosten verbunden gewesen wäre.[164] Tatsächlich gab es schon nach wesentlich kürzerer Zeit Schwarzseher-Lösungen. Bei der Verschlüsselungsumstellung von Betacrypt auf Nagravision im Jahr 2003 rechnete man bei Premiere nur noch mit einem Zeitraum von einem Jahr, bis das System geknackt würde. Allerdings ist auch nach über einem Jahr noch keine praktikable Schwarzseherlösung gefunden worden.[165] Ebenso wenig kann präzisiert werden, wie hoch die Einnahmen sind, die sich auf die umgehungssichere Verschlüsselung zurückführen lassen. Daher müssen Schätz- und Erwartungswerte als Grundlage dienen. Erwartungswerte müssen zu Beginn der Betrachtungsperiode auch für die Einnahmen aus der Vermietung und dem Verkauf von Decodern, die Erträge aus Kautionsbeträgen und die Aktivierungsgebühren gebildet werden, diese können jedoch im Laufe der Betrachtungsperiode tatsächlich gemessen werden und für künftige Prognosewerte als Grundlage dienen.

3.4. Technische Maßnahmen gegen Schwarzseher

Sobald eine Verschlüsselung geknackt ist, versuchen die Pay-TV-Anbieter die Möglichkeiten des Schwarzsehens zu unterbinden, um Einnahmeverluste zu vermeiden. Ein Versuch, den Schwarzsehern den illegalen Fernsehgenus zu

---

[163] Vgl. o.V., o.J.(21).

[164] Hunsel, 1991, S. 56

[165] Hankmann, Sprotte, 2004e

verleiden, ist die regelmäßige Änderung der Verschlüsselungscodes. Piratenkarten werden dadurch unbrauchbar und müssen vor einer weiteren Nutzung erst mit einem Update versehen werden. Da nach Hochrechnungen von Premiere mehr als 90 Prozent der Schwarzseher über keine oder nur geringe Technikkenntnisse verfügen, können sie das Update nicht selbst vornehmen, sondern müssen dieses unter Kosten- und Zeitaufwand extern durchführen lassen. Durch häufige Codeänderungen und dadurch erforderliche Updates sollen die Schwarzseher demoralisiert werden und das Schwarzsehen aufgeben.[166] Verfügt jedoch ein Schwarzseher über entsprechende Kenntnisse und das notwendige Computer-Equipment, kann er die neuen Codes einfach aus dem Internet laden, die schon nach weniger als einer Stunde nach dem Codewechsel bereit stehen können.[167]

Auf eine zeitliche Zugangsbeschränkung setzen einige Anbieter, die ihr Programm ausschließlich über Satellit verbreiten. Mit dem Kauf einer Karte gegen eine einmalige Zahlung kann der Zugang zu dem Programm nur für einen limitierten Zeitraum erworben werden, beispielsweise für sechs oder zwölf Monate. Nach Ablauf dieser Zeit muss dann eine neue Smartcard mit aktuellem Code gekauft werden.[168]

Eine drastischere Konsequenz ist der Wechsel des gesamten Verschlüsselungssystems. Dies kann durch den Austausch sämtlicher Smartcards erfolgen und wurde in der Vergangenheit von verschiedenen Sendern bereits durchgeführt. Zum Beispiel stellte Premiere, wie bereits erwähnt, im Jahr 2003 von Betacrypt auf Nagravision2/Aladin um.[169] Auf das gleiche System wechselte im März 2004 Digital+ in Spanien[170], da es bislang als piratensicher gilt. In Skandinavien stellt Viasat zur Zeit von Viaccess 1 auf Videoguard um.[171] In Malaysia entdeckte letztes Jahr der Kabelsender Astro Kopien seiner digitalen Smartcards und sah sich daraufhin gezwungen, sein gesamtes System neu aufrüsten.[172]

3.4.1. Kosten einer Verschlüsselungsumstellung

Da jedes Codiersystem früher oder später angreifbar durch Piraterie wird, ist es notwendig, dieses alle paar Jahre durch ein System zu ersetzen, welches technisch auf dem neuesten Stand ist.[173] Eine vollständige Umstellung des Verschlüsselungssystems ist mit hohem Aufwand und Kosten verbunden. Bran-

---

[166] Hofmeir, 2003b

[167] o.V., 2002(16)

[168] Posewang, 2004, S. 39

[169] o.V., 2003(10)

[170] o.V., 2004(4)

[171] Hagedorn, 2004a, S. 21

[172] Schubert, 2004b

[173] o.V., o.J.(21)

cheninternen Informationen zufolge entstehen bei einem Smartcard-Tausch pro Karte Kosten in Höhe von ca. 11,- Euro.[174]

Sky Italia musste bei einer Verschlüsselungsumstellung sämtliche 1,9 Millionen Kunden mit neuen Smartcards für Videoguard versorgen. Basierend auf den Umtauschkosten pro Karte in Höhe von 11,- Euro entstanden dem Sender hierfür 20,9 Millionen Euro an Kosten. Damit die vorhandenen Decoder-Boxen auch für Videoguard geeignet sind, musste ein Software-Upgrade bei jedem Abonnenten durchgeführt werden, welches zusätzliche Kosten verursachte. In Fällen, in denen dies nicht möglich war, wurde die Box durch Sky Italia kostenlos ausgetauscht.

Als Premiere am 1. November 2003 die Umstellung seines Verschlüsselungssystems von Betacrypt zur aktuellen Nagravision-Version durchführte, mussten über 2,7 Millionen neue Smartcards an die Abonnenten verschickt werden[175]. Werden Umtauschkosten von 11,- Euro pro Karte zugrunde gelegt, entstanden allein für den Smartcard-Tausch Kosten in Höhe von 29,7 Millionen Euro. Die Vorbereitungszeit für die Umstellung betrug mehr als ein Jahr. Zunächst wurden alle großen Verschlüsselungssysteme wie Irdeto, Mediaguard, NDS und Nagravision getestet.[176] Nachdem die Wahl schließlich auf Nagravision gefallen war, erarbeitete Premiere gemeinsam mit Nagravision einen Anforderungskatalog. Die Ausarbeitungen nahmen einige Monate in Anspruch. Die vertraglichen Vereinbarungen waren sehr komplex und umfassten einen ganzen Aktenordner.[177] Ausschlaggebend für die Wahl eines geeigneten Systems war neben der Sicherheit die Kompatibilität mit den bereits bei den Kunden vorhandenen Decoderboxen. Schließlich wollte man mit der Umstellung die Schwarzseher, nicht jedoch die zahlenden Kunden verärgern. Sie sollten lediglich ihre neue Smartcard gegen die alte austauschen müssen. Nur für die wenigen Nutzer eines Premiere CI-Moduls wurde zusätzlich ein Software-Update via Satellit notwendig.[178] Nach Vertragsabschluß wurde die Produktion der neuen Smartcards bei Nagravision gestartet. Anschließend wurde ein interner Feldversuch durchgeführt, bei dem auch die Sicherheit getestet wurde. Gleichzeitig wurden Gespräche mit Herstellern von Decoderboxen geführt, um möglichst schnell günstige Premiere-Receiver mit dem neuen Verschlüsselungssystem auf den Markt zu bringen. Die produzierten Smartcards lieferte Nagravision an Premiere, anschließend verschickte Premiere sie an die Abonnenten.[179] Der Versand der Smartcards erfolgte in neutralen Umschlägen, um dem Diebstahl von Karten vorzubeugen. Wird von der Standardfrankierung eines Briefes in Höhe von 55 Cent pro Brief ausgegangen, fielen bei 2,7 Millionen Sendungen Kosten von 1.485.000,- Euro nur für das Porto an. Zusätzlich musste damit gerechnet wer-

---

[174] o.V., 2002(4) S. 6

[175] Fiutak, 2003

[176] Goedecke, Hofmeir, 2003c, S. 23 f.

[177] dies., 2003a, S. 12

[178] dies., 2003c, S. 23f.

[179] dies., 2003a, S. 12

den, in einigen Fällen Ersatzkarten zu verschicken, wenn die erste Sendung bei den Kunden nicht ankam. Mit dem Versand der Karten wurde ein externer Dienstleister beauftragt, der ebenfalls entlohnt werden musste.[180]

Die Entwicklung eines neuen CA-Systems dauert ungefähr zwei Jahre und kostet zwischen 20 und 30 Millionen Euro. In der Zwischenzeit wird auch die Computertechnologie aufgrund äußerst kurzer Innovationszyklen immer leistungsfähiger bei gleichzeitig fallenden Preisen. Von dieser Entwicklung profitieren jedoch in erster Linie nicht die Entwickler der Codierungssysteme, sondern die Hacker, die auf diese Weise stets über neueste und leistungsfähige Technologie verfügen, mit der sie auch immer ausgefeiltere Verschlüsselungssysteme knacken können.[181]

3.4.2. Nutzen der Verschlüsselungsumstellung

Von der Umstellung des Verschlüsselungssystems versprechen sich die Sender, alle Schwarzseher zumindest vorübergehend ausschließen zu können, da die Piratenkarten zum Umstellungszeitpunkt wirkungslos werden.[182] Wie lange es dauert, bis auch eine neue Verschlüsselung geknackt wird, ist nicht vorhersehbar. Premiere-Chef Georg Kofler ging beim Wechsel von Betacrypt zu Nagravision im September 2003 davon aus, dass es auch für das neue System bereits nach einem Jahr Piratenkarten geben werde.[183] Vorsorglich hat Premiere mit der Kudelski Gruppe, zu der Nagravision gehört, vertraglich einen Schadenersatzanspruch vereinbart, falls die Verschlüsselung massenhaft geknackt werden sollte.[184] Im Oktober 2004 sieht der Leiter von Premieres Abteilung „E-Security“ jedoch immer noch keinen stichhaltigen Hinweis auf einen erfolgreichen Hack und geht davon aus, dass es noch für lange Zeit keine Piratenkarte für Nagravision geben wird.[185] Weniger Glück hatte dagegen der italienische Sender Stream. Er wechselte im Jahr 2003 von den beiden verwendeten Codierungen Irdeto 1 und Seca/Mediaguard 1 zu Mediaguard 2, da für die ursprünglichen Verschlüsselungen enorm große Mengen an Piratenkarten gehandelt wurden. Stream musste jedoch bereits nach kurzer Zeit feststellen, dass auch Mediaguard 2 durch Piraten geknackt worden war, so dass sich der Sender 2004 erneut gezwungen sah, eine Umstellung vorzunehmen, dieses Mal auf Videoguard. [186]

Für die Sender ist es wichtig zu signalisieren, dass gegen das Schwarzsehen vorgegangen wird. Dies soll zum einen bisherige Schwarzseher von zukünftigem illegalen Genuss abhalten und sie dazu motivieren, sich einen legalen Zu-

---

[180] dies., 2003c, S. 23f.

[181] o.V., 2003(8)

[182] Vgl. Fiutak, 2003

[183] Hankmann, Sprotte, 2004e

[184] Goedecke, Hofmeir, 2003c, S. 24

[185] Hankmann, Sprotte, 2004e

[186] Hagedorn, 2004a, S. 21

gang zu beschaffen, der nicht immer wieder durch Wechsel der Codes abgeschaltet wird, zum anderen sollen auch die legalen Nutzer davon abgehalten werden, zukünftig selbst zu Schwarzsehern zu werden. Wenn Blanko-Smartcards für ca. fünf Euro und die notwendige Software gratis im Internet zu erhalten sind, stellen sich zunehmend auch ehrliche Pay-TV Kunden die Frage, warum sie Gebühren von 30 Euro und mehr pro Monat bezahlen sollen. Bleibt ein Sender untätig gegenüber dieser Bedrohung, gefährdet er seine Existenzgrundlage.[187] Daher muss auch den Bestandskunden vermittelt werden, dass Schwarzsehen mit Ärger durch Abschaltungen aufgrund regelmäßiger Codeänderungen und mit enormem Aufwand durch das Finden und Installieren von neuer Cracksoftware oder der kostspieligen Beschaffung neuer illegaler Smartcards verbunden ist. Durch eine Verschlüsselungsumstellung möchten die Pay-TV-Anbieter eine Verkleinerung des Absatzpotentials und Kundenrückgang vermeiden. Gleichzeitig versprechen sich die Sender, dass bisherige Schwarzseher durch die Abschaltung ihres illegalen Zugangs motiviert werden, reguläre und damit bezahlende Kunden zu werden. Falls die illegalen Zuschauer nicht mehr auf das Pay-Programm verzichten wollen und eine Zahlungsbereitschaft entwickelt haben, die zuvor nicht vorhanden war, kann auf diese Weise sogar das Absatzpotential vergrößert werden. Premiere-Chef Kofler setzte bei der letzten Verschlüsselungsumstellung genau auf diesen Effekt, indem er erwartete, dass einige hunderttausend Schwarzseher zu regulären Abonnenten würden.[188] Er verwies dabei auf Erfahrungen aus dem Ausland, wo bis zu 50 Prozent der Schwarzseher nach einer Verschlüsselungsänderung zu Neuabonnenten geworden wären. Beispielsweise konnte der italienische Pay-TV-Anbieter Telepiu nach einer Umstellung des Verschlüsselungssystems innerhalb von drei Monaten einen Zuwachs von 240.000 Abonnenten verzeichnen.[189] In Deutschland bestätigten sich Koflers Erwartungen jedoch nicht, nur etwa zehntausend Neuabschlüsse wurden kurz nach der Umstellung getätigt.[190]

3.4.3. Kosten-Nutzen-Abwägung der technischen Schwarzseherbekämpfung

Damit die Umstellung des Verschlüsselungssystems eine rationale Entscheidung ist, muss der Nutzen aus der Verschlüsselungsumstellung höher sein als die dadurch entstehenden Kosten.

Die bei einer Verschlüsselungsumstellung entstehenden Kosten entsprechen weitgehend denen des Verschlüsselungssystems, die in Kapitel 3.3.7. dargestellt wurden. Für die neue Verschlüsselung ist ein Kaufpreis zu entrichten, zu dem auch die Transaktionskosten für die Auswahl eines geeigneten Systems bis zum Vertragsabschluß und dessen Kontrolle sowie eventueller Nachbesserungen hinzuzurechnen sind. Wird ein eigenes System entwickelt, müssen hier-

---

[187] Vgl. Goedecke, Hofmeir, 2003c, S. 23.

[188] Ein Premiere-Sprecher erwartete, daß sicherlich 200.000 Schwarzseher zu Premiere-Abonnenten werden. Siehe hierzu Herres, 2003, S. 12.

[189] o.V., 2002(14)

[190] Müller, 2003

für die Entwicklungskosten kalkuliert werden. Sowohl beim Zukauf als auch bei der Eigenentwicklung fallen Kosten für die Implementierung des Systems einschließlich aller notwendigen Tests an. Hinzu kommen Kosten für neue Decoder, falls sie erforderlich werden, und deren notwendige Zertifizierung für das neue Codiersystem. Zusätzlich müssen die Kosten des Versands der neuen Smartcards an jeden Bestandskunden einkalkuliert werden, die im Regelfalle der Pay-TV-Anbieter übernimmt, um die zahlenden Abonnenten nicht zu verärgern. Wird ein Softwareupgrade der Kunden-Decoder notwendig, entstehen Kosten für die dafür notwendige Software. Die Durchführung des Upgrades kann unkompliziert und kostengünstig per Satellit oder Kabel erfolgen; sofern dies nicht möglich ist, muss ein Decoderaustausch beim Kunden erfolgen. Werden diese Kosten ebenfalls nicht den betroffenen Kunden angelastet, entstehen dem Pay-TV-Sender Kosten für die Beschaffung der neuen Decoder und die Zustellung an den Kunden. Während der Nutzungsdauer entstehen die Kosten des laufenden Betriebs. Darüber hinaus sind die Finanzierungskosten der Umstellung zu berücksichtigen. Es ergibt sich folgende Kostengleichung:

$$K_{VU} = K_{KV} + K_{EV} + K_{IV} + K_{ZD} + K_{DS} + K_F + K_{VS} + K_{DU} + K_{VAD} + K_{BV} ,$$

mit:

K_{VU}: Gesamtkosten der Verschlüsselungsumstellung

K_{KV}: Kosten des Kaufs eines neuen Verschlüsselungssystems

K_{EV}: Kosten der Eigenentwicklung eines neuen Verschlüsselungssystems

K_{IV}: Kosten für die Implementierung des neuen Verschlüsselungssystems

K_{ZD}: Kosten für die Zertifizierung von Decodern

K_{DS}: durchschnittliche Kosten innerhalb der Zeitperiode T für die Beschaffung der Decoderboxen und Smartcards für die Abonnenten inkl. Lagerkosten und Verzinsung bis zur Auslieferung

K_F: Kosten für die Finanzierung der Verschlüsselungsumstellung

K_{VS}: Kosten für den Versand der neuen Smartcards

K_{DU}: Kosten für Decoderupgrades

K_{VAD}: Kosten für den Versand der Austauschdecoder

K_{BV}: Kosten für den laufenden Betrieb des neuen Verschlüsselungssystems während des Betrachtungszeitraums T.

Die Kosten des Versands der neuen Smartcards setzen sich aus den Kosten des Briefversands (Kosten für Briefumschläge und Porto einschließlich eventueller Versand-Versicherungsprämien) und den Personalkosten der beteiligten Mitarbeiter zusammen. Wird der Versand durch einen externen Dienstleister vorgenommen, ist dieser anstatt der eigenen Mitarbeiter zu entlohnen. Die Gleichung lautet:

$$K_{VS} = K_B * x_{RA} + k_p/t * M * T_{VS} ,$$

mit

K_B: Kosten pro Brief (Briefumschlag + Porto + Versicherung)

x_{RA}: Anzahl aller registrierten Abonnenten zum Zeitpunkt der Verschlüsselungsumstellung

T_{VS}: Zeitraum des Versendens aller Austausch-Smartcards.

Die Kosten für das Decoderupgrade bestehen aus den Kosten für die Upgrade-Software und den Arbeitskosten der Upgrade-Durchführung:

$K_{DU} = K_{US} + k_p/t * M * T_U$,

mit

K_{US}: Kosten für die Beschaffung der Upgrade-Software

T_U: Zeitraum der Durchführung des Upgrades.

Der Versand von Austausch-Decodern verursacht Kosten für das Versandpaket, bestehend aus dem Verpackungsmaterial, dem Porto einschließlich eventueller Prämien für die Versand-Versicherung, und den dafür anfallenden Arbeitskosten. Auch hier sind bei Inanspruchnahme eines externen Dienstleisters dessen Kosten anstatt der eigenen Lohnkosten anzusetzen. Es ergibt sich folgende Gleichung:

$K_{VAD} = K_P * x_{AD} + k_p/t * M * T_{VAD}$,

mit

K_P: Kosten pro Versandpaket (Verpackungsmaterial + Porto + Versicherung)

x_{AD}: Anzahl der Kunden, die einen Austausch-Decoder benötigen

T_{VAD}: Zeitraum des Versendens aller Austausch-Decoder

Die Kosten der Austausch-Decoder selbst sind in den Anschaffungskosten der Decoder K_{DS} mit einzukalkulieren. Sofern die Decoder kostenlos an die Kunden gegeben werden, stehen diesen Kosten jedoch keine Einnahmen gegenüber.

Die Kosten sind gegenüber dem Nutzen der neuen Verschlüsselung in Form von Einnahmen abzuwägen. Diese bestehen aus den Einnahmen durch die Sicherung des Kundenbestands und des Absatzpotentials, in dem zahlungsbereite Kunden vom Schwarzsehen abgehalten und gegebenenfalls als Abonnenten wieder zurückgewonnen werden, und aus den Einnahmen einer Kundenbestands- und Absatzpotentialerweiterung, welche aus bisherigen Schwarzsehern resultiert, die bisher keine Kunden waren, jedoch nicht mehr auf das Pay-TV-Programm verzichten wollen und zu zahlenden Abonnenten werden. Zu der Erweiterung trägt zusätzlich auch hier die Steigerung der Programmqualität durch die Erhöhung der Einnahmen bei. Die übrigen Einnahmen, die durch Zinserträge der angenommenen Kautionen für Smartcards und Decoder, aus dem Verkauf oder der Vermietung von Decodern und Aktivierungsgebühren oder anderen Einmalzahlungen generiert werden, entstehen ebenfalls bei dem neuen Verschlüsselungssystem.

$N_{VU} = E_{SKA} + E_{EKA} + E_{KS} + E_{KD} + E_{DV} + E_{DM} + E_A$,

mit:

N_{VU}: Nutzen, der aus der Umstellung des Verschlüsselungssystems resultiert

E_{SKA}: Einnahmen durch Abonnementgebühren von Kunden, die nur aufgrund mangelnder Schwarzseh-Optionen zahlende Abonnenten sind (Sicherung des Kundenbestands und des Absatzpotentials durch Verschlüsselung)

E_{EKA}: Einnahmen durch Abonnementgebühren ehemaliger Schwarzseher und von Neuabonnenten durch gesteigerte Programmqualität

E_{KS}: Einnahmen durch Zinserträge aus den Smartcard-Kautionsbeträgen

E_{KD}: Einnahmen durch Zinserträge aus den Decoder-Kautionsbeträgen

E_{DV}: Einnahmen aus dem Verkauf von Decodern

E_{DM}: Einnahmen aus der Vermietung von Decodern

E_A: Einnahmen aus Aktivierungs- oder Freischaltgebühren oder ähnlichen Einmalzahlungen.

Die Berechnung der Einnahmen als Folge der Kundenbestandserweiterung ist bei der Verschlüsselungsumstellung zu ergänzen und stellt sich folgendermaßen dar:

$$E_{EKA} = ARPU/t * (x_{EKM} + x_{SCH}) * T ,$$

mit

x_{EKM}: durchschnittliche Anzahl der Abonnenten, die im Zuge der Absatzpotentialerweiterung aufgrund der Programmqualitätsverbesserung zu zahlenden Kunden werden und zuvor keine Schwarzseher waren

x_{SCH}: durchschnittliche Anzahl der Schwarzseher, die noch nie Abonnenten waren, nach dem Ausschluss durch die neue Verschlüsselung jedoch nicht mehr auf das Pay-TV-Programm verzichten wollen und zu zahlenden Abonnenten werden.

Die übrigen Einnahmen lassen sich analog zu Kapitel 3.3.7. ermitteln.

Damit eine Verschlüsselungsumstellung aus ökonomischer Sicht rational ist, muss der Nutzen, der sich durch die Umstellung erzielen lässt, höher sein als die Kosten, die aus der Maßnahme resultieren:

$$N_{VU} > K_{VU} .$$

Die Entwicklung eines komplett neuen CA-Systems kostet zwischen 20 und 30 Millionen Euro.[191] Wird angenommen, dass das System an mehrere Pay-TV-Sender verkauft wird, kann der Kaufpreis für ein solches System auf fünf bis zehn Millionen Dollar geschätzt werden. Diese Kosten, die sich um die übrigen Kosten für Implementierung, Betrieb etc. erhöhen, müssen während der Nutzungszeit des Verschlüsselungssystems erwirtschaftet werden.

Einige Sender ignorieren die Tatsache, dass ihr verwendetes Verschlüsselungssystem geknackt und durch illegale Zugangssysteme unterlaufen ist und unternehmen keine Umstellungsbemühungen. Beispielsweise verwendet der niederländische Sender Canal Digitaal für seine Inlandsprogramme das System Irdeto 1 und möchte es auch in Zukunft beibehalten, obwohl es keine sichere

[191] o.V., 2003(8).

Verschlüsselung mehr gewährleistet.[192] Möglicherweise sieht der Sender in einer Verschlüsselungsumstellung kein angemessenes Kosten-Nutzen-Verhältnis, statt dessen erscheinen Kosten/Nutzen des status quo für ihn attraktiver.

In einer Hinsicht erweisen sich technische Bekämpfungsmaßnahmen wie Verschlüsselungsumstellungen jedoch als kontraproduktiv: Wird das Pay-TV-Programm im Ausland, in dem ein legaler Empfang nicht möglich ist, mittels Piratentechnik empfangen, müssen sich die Interessenten nach der Abschaltung mangels legaler Alternative erneut an die Piraten wenden. Auf diese Weise erfolgt statt einer Bekämpfung eine Förderung des Piraterie-Marktes.[193]

3.5. Direkte Bekämpfung der Pay-TV-Piraten

Dem Problem der Piraterie ist allein mit technischen Mitteln nicht ausreichend beizukommen, auch weiterentwickelte und aufwendige Verschlüsselungstechniken bieten auf längere Sicht keinen hundertprozentigen Schutz vor illegaler Entschlüsselung. Zusätzlich sind daher Anstrengungen erforderlich, die der direkten Bekämpfung von Hackern und Dealern der Piratentechnik dienen.[194]

3.5.1. Maßnahmen der direkten Bekämpfung von Pay-TV-Piraten

Zur Bekämpfung der Piraterie wird in der Branche ein dreigleisiger Ansatz verfolgt. Neben der ständigen Verbesserung der Verschlüsselungstechnologie führen die Anbieter von Pay-TV und Verschlüsselungssystemen eigenständige Recherchen mit privaten Ermittlern durch. Zusätzlich halten die betroffenen Firmen, dazu zählen neben den Pay-TV-Anbietern z.B. auch die Hersteller von Decoderboxen, untereinander und mit internationalen Stellen Kontakt und pflegen eine enge Zusammenarbeit. Viele von ihnen sind Mitglieder der Organisationen STOP oder AEPOC.

STOP steht für „Scandinavian TV Organisation Against Piracy“ und ist ein freiwilliger Zusammenschluss skandinavischer Fernsehsender, um gemeinsam gegen Piraterie vorzugehen. Nach Gründung Ende der neunziger Jahre hat sich STOP mittlerweile zu einem wirkungsvollen Forum mit gesamteuropäischer Beteiligung entwickelt. Der Organisation gehören Unternehmensvertreter und -anwälte an, um mit legalen Mitteln gemeinsam gegen Piraten vorzugehen. Neben den skandinavischen verfügt STOP auch über Mitglieder aus Deutschland, England, Italien, Frankreich, den Niederlanden, Belgien und Island.[195] Die AEPOC („Association Européenne pour la Protection des Œuvres et Services Cryptés“) ist eine europäische Vereinigung zum Schutz verschlüsselter Dienste, deren Ziel die Beseitigung der Piraterie und die Verbesserung der technologischen und juristischen Rahmenbedingungen zum Schutz der verschlüsselten

---

[192] Hagedorn, 2004b, S. 20

[193] o.V., 2003(3), S. 23

[194] Vgl. Lievaart, 2001, S. 2.

[195] o.V., 2002(10)

Dienste ist. Ihr gehören 35 Mitglieder an, zu denen unter anderen Anbieter von Pay-TV und Verschlüsselungstechnik zählen.[196]

Betriebsintern hat der deutsche Pay-TV-Anbieter Premiere für die Bekämpfung der Schwarzseher eine eigene Abteilung eingerichtet, die sich Premiere E-Security nennt und sowohl Juristen als auch Techniker beschäftigt.[197] Diese ermitteln eigenständig und gehen gegen Schwarzseher, Entwickler von Piratensoftware und Dealer von Piraten-Equipment auch gerichtlich vor. Zusätzlich schult die Abteilung deutschlandweit Kriminalpolizei und Rechtsanwälte[198] und unterstützt Polizei und Staatsanwaltschaften bei ihren Ermittlungen.[199] Auch die Firma Irdeto Access, weltweit tätig im Bereich Schutz und Management von Inhalten, verfügt über eine eigene Sicherheitsabteilung. Deren Ermittlungen, die auch in Zusammenarbeit mit Unternehmen wie Premiere durchgeführt werden, führten in der Vergangenheit bereits zu erfolgreichen Polizeirazzien, bei denen illegal programmierte Smartcards für diverse europäische Pay-TV-Sender, Pirateriesoftware, Dateien mit geheimen Schlüsseln, CA-Module mit entsprechenden Geräten zur illegalen Softwarebestückung und weiteres Piraten-Equipment sichergestellt werden konnten.[200] Irdeto unterstützt ebenfalls die lokalen Strafverfolgungsbehörden mit Dossiers über neueste Erkenntnisse und liefert ihnen Beweismaterial, die zur Ergreifung von Piraten führen.[201] Zu den Ermittlungen gehören auch Recherchen im Internet. Pay-TV-Sender und Firmen aus dem Hersteller-Bereich wie der Smartcard-Produzent SCM kontrollieren beispielsweise auch Online-Auktionshäuser wie ebay nach Angeboten von Piraterie-Produkten. Firmen wie Premiere oder SCM haben bei ebay Zugriff auf das sogenannte „Verifizierte Rechte Inhaber Programm“ (VeRI), mit dem sie unmittelbar bestimmte Auktionen löschen können. Innerhalb von 10 Monaten wurden auf diese Weise 5.000 Auktionen aus dem ebay-Angebot entfernt.[202]

Neben den Pay-TV-Sendern und den Anbietern der Verschlüsselungstechnik engagieren sich auch Hersteller von Decoderboxen aktiv für die Bekämpfung der Piraterie. Beispielsweise sieht Humax, Hersteller von Digitalboxen, als Folge des Pay-TV-Hackens eine Bedrohung für den gesamten Digital-TV-Markt und damit auch die eigenen Umsatzziele in Gefahr. Durch die Eindämmung der Piraterie will Humax die finanzielle Kraft der Pay-TV-Sender stärken, so dass sie in ein qualitativ höherwertiges Programmangebot investieren können und dadurch mehr Kunden gewinnen. Mit jedem verkauften Abonnement wird dann auch eine Digitalbox verkauft. Bekämpfungsmaßnahmen umfassen die Absicherung der Boxen durch Spezialversiegelungen, proaktives Vorgehen gegen die Verbreitung illegaler Inhalte im Internet unter Ausschöpfung aller juristischen

---

[196] o.V., 2004(13)

[197] Hofmeir, 2003b

[198] ebenda, S. 16

[199] o.V., 2002(15)

[200] o.V., 2002(10)

[201] o.V., o.J.(10)

[202] Hofmeir, 2003b

Mittel und die Einstellung des Verkaufs aller manipulierbaren Boxen, auch wenn diese umsatzstark sind.[203] Darüber hinaus beteiligt sich Humax, genauso wie Premiere, SCM oder Irdeto, als Mitglied bei der AEPOC.[204]

Außer der Aneignung genauer Kenntnisse der juristischen Möglichkeiten, mit denen gegen die Piraterie vorgegangen werden kann, müssen die Pay-TV-Anbieter intensive Lobbyarbeit bei Behörden und in der Politik betreiben, um bestehende rechtliche Defizite zu beseitigen, die die Bekämpfung der Piraterie erschweren oder behindern. Erfolgreiche Lobbyarbeit der AEPOC bewirkte bereits den Erlass einer Direktive[205] durch das Europäische Parlament und den Rat der Europäischen Union, welche Piraterie-Aktivitäten wie Herstellung, Import, Distribution, Verkauf, Vermietung, Besitz, Wartung oder Austausch von Vorrichtungen für die unberechtigte Decodierung zu kommerziellen Zwecken in den EU-Staaten sanktioniert.[206] Umgesetzt wurde diese Richtlinie in Deutschland mit dem Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (Zugangskontrolldiensteschutz-Gesetz – ZKDSG).[207]

3.5.2. Kosten-Nutzen-Abwägung der direkten Bekämpfung

Kosten der direkten Bekämpfung von Pay-TV-Piraten werden vor allem durch innerbetriebliche Aktivitäten, durch extern durchgeführte Schulungen z.B. bei Behörden und Anwälten und durch die Unterstützung überbetrieblicher Organisationen verursacht:

$K_{APB} = K_{IM} + K_{ESM} + K_{UO}$,

mit

K_{APB} : Kosten für die aktive Piraten-Bekämpfung

K_{IM} : Kosten für innerbetriebliche Maßnahmen

K_{ESM} : Kosten für externe Schulungsmaßnahmen bei Behörden, Anwälten etc.

K_{UO} : Kosten für die Unterstützung von überbetrieblichen Organisationen.

---

[203] Pötzsch, 2002

[204] o.V., 2004(3)

[205] Richtlinie 1998/84/EG des Europäischen Parlaments und des Rates über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten vom 20. November 1998 (ABl. L 320 vom 28. November 1998, S. 54). Ziel der Direktive ist die Angleichung der Rechtsvorschriften der Mitgliedsstaaten bzgl. der Maßnahmen gegen illegale Vorrichtungen für den unerlaubten Zugang zu geschützten Diensten. Siehe hierzu: Laga, 1999, S. 3.

[206] Lievaart, 2001, S. 2

[207] Bundesgesetzblatt Jahrgang 2002 Teil I Nr. 19, ausgegeben zu Bonn am 22. März 2002, Seite 1090

Als Nutzen stehen diesen Kosten die vermiedenen Einnahmeausfälle gegenüber, die aus der erfolgreichen Bekämpfung der Pay-TV-Piraterie resultieren:

$N_{APB} = E_{VPA}$,

mit

N_{APB} : Nutzen der aktiven Piraten-Bekämpfung

E_{VPA} : verhinderte Einnahmeausfälle durch vermiedene Piratenaktivitäten.

Das wirtschaftliche Ziel muss sein, dass der Nutzen die Kosten der aktiven Piraten-Bekämpfungsmaßnahmen übertrifft:

$N_{APB} > K_{APB}$.

In den für die Piraterie-Bekämpfung zuständigen Abteilungen der Pay-TV-Sender werden Spezialisten benötigt, die über (Computer-)technisches und juristisches Wissen sowie kriminalistische Fähigkeiten verfügen. Eine wichtige Aufgabe der Abteilung ist die Ermittlungsarbeit. In einem sich schnell ändernden und undurchsichtigen Umfeld der Illegalität wie der Pay-TV-Piraterie-Szene ist es erforderlich, dass die Unternehmen stets auf dem neuesten Stand sind. Die Mitarbeiter müssen sich also laufend aus aktuellen Quellen über die Entwicklung der Piraterie-Aktivitäten informieren. Eine gute Quelle bietet hier das Internet. In speziellen Foren oder Newsgroups tauschen sich Hacker und Schwarzseher über die neuesten Methoden und Bezugsquellen aus. Oft sind diese Informationsplattformen jedoch nicht leicht ausfindig zu machen, beispielsweise über Suchmaschinen, da Schlüsselworte wie „hacken“ oder „geknackt“ nicht ausgeschrieben, sondern abgekürzt oder durch Symbole verfremdet dargestellt werden (z.B. anstelle von „geknackt“ nur „gek***t“).[208] Diese Art der Informationsbeschaffung ist daher mit einem hohen Zeit- und damit Kostenaufwand verbunden. Zusätzlich müssen Internetplattformen wie das virtuelle Auktionshaus ebay regelmäßig nach Anbietern von Piraterie-Technik durchsucht werden. Die Angebote ändern sich permanent, von daher ist eine häufige Kontrolle notwendig. Werden illegale Angebote entdeckt, müssen die Anbieter gefunden und rechtliche Maßnahmen gegen sie geprüft werden. Werden Hacker oder Dealerringe ausfindig gemacht, werden die öffentlichen Behörden wie Polizei und Staatsanwaltschaft eingeschaltet. Aus diesem Grund ist eine permanente Kontaktpflege zu den Behörden einschließlich regelmäßiger Schulungsangebote unerlässlich, damit im Ernstfall ohne große Zeitverzögerung auf die Behördenunterstützung zurückgegriffen werden kann. Kosten entstehen für diese Maßnahmen also in erster Linie in Form von Personalkosten, die mit der aufwendigen Informationsbeschaffung, der Informationsversorgung der Behörden und der Planung und Durchführung von Bekämpfungsmaßnahmen wie z.B. der Erstattung von Anzeigen verbunden sind.

[208] Vgl. Hankmann, Sprotte, 2004c, S. 88.

Pro bearbeitetem Fall entstehen dann folgende Arbeitskosten:

$K_{IM} = k_p/t * M * T$,

mit

T: Gesamtdauer eines bearbeiteten Falls

Sind in der Abteilung beispielsweise zehn Mitarbeiter beschäftigt, deren einzelne Stelle im Durchschnitt pro Jahr 100.000,- Euro Kosten verursacht, entstehen dem Unternehmen Kosten von einer Million Euro pro Jahr. Werden durch die Ermittlungen Erfolge erzielt, die Schaden vom Unternehmen von mehr als einer Million Euro pro Jahr abwenden, etwa durch die Ergreifung von Kartendealern, durch die Aufdeckung von Dealerringen oder durch die Abschreckung von Piraten, steht dem Einsatz der Abteilung eine positive Kosten-Nutzen-Bilanz gegenüber.

Auch die Unterstützung von Organisationen und Interessenverbänden wie der AEPOC oder STOP ist mit Kostenaufwand, insbesondere in Form von Mitgliedsbeiträgen[209], Zeitaufwand entsendeter Mitarbeiter zu Veranstaltungen, Zeitaufwand für den Informationsaustausch etc. und anfallenden Reisespesen verbunden:

$K_{UO} = K_{MB} + k_p/t * M * T + K_{RS}$,

mit

K_{MB} : Kosten für Mitgliedsbeiträge

K_{RS}: Kosten für Reisespesen

T: Gesamtdauer der durchgeführten Mitglieds-Aktivitäten

Diesen Kosten steht der Nutzwert des Engagements gegenüber, der in dem verhinderten Schaden des Pay-TV-Senders durch Erfolge der Organisationen gegen die Pay-TV-Piraterie besteht. Werden z.B. durch die Zusammenarbeit der Mitglieder Erfolge gegen die Pay-TV-Piraterie erzielt, die einen Pay-TV-Sender vor einem jährlichen Schaden in Höhe von einer Million Euro bewahren, hätte sich ein eingesetzter Gesamtbetrag des Senders von weniger als einer Million Euro pro Jahr für das Engagement in der Organisation rentiert. Wird der Wert des durchschnittlichen Umsatzes pro Kunde (ARPU) von 260,40 Euro im Jahr angesetzt, wäre der AEPOC-Mitgliedsbeitrag in Höhe von 7000,- Euro bereits dann gerechtfertigt, wenn durch das Engagement der Organisation 27 Schwarzseher pro Jahr vermieden würden, die einen jährlichen wirtschaftlichen

[209] Beispielsweise verpflichten sich die Mitglieder der AEPOC gemäß der Satzung, einen jährlichen Mitgliedsbeitrag zu zahlen, dessen Höhe jedes Jahr neu festgelegt wird (o.V., o.J.(4)). Der Beitrag beträgt nach Auskunft der AEPOC derzeit für Vollmitglieder 7000 Euro pro Jahr. Vollmitglieder besitzen Wahl- bzw. Abstimmungsrechte. Unternehmen außerhalb der EU können außerordentliche Mitglieder („Associate“) werden. Sie besitzen keine Wahl- und Abstimmungsrechte und entrichten keine Mitgliedsgebühr. Alle Mitglieder können an Sitzungen (board meetings, general assemblies) teilnehmen und kommen in den Genuß des Netzwerks und des hierin stattfindenden Informationsaustausches (Schembri, 2005).

Schaden durch Nicht-Entrichtung der Pay-TV-Gebühren von 7030,80 Euro[210] verursacht hätten.

Da es sich bei der Piraterie, auch im Pay-TV-Bereich, um ein länderübergreifendes Problem handelt, ist insbesondere auch ein Engagement in den internationalen Organisationen sinnvoll. Soft- und Hardware für die Umgehung der Verschlüsselungen werden von Hackern in verschiedenen Ländern hergestellt und grenzübergreifend vertrieben. Dabei kommt den Hackern entgegen, dass die gleichen, ggf. mit einigen Modifikationen versehenen, Verschlüsselungen von verschiedenen Sendern in diversen Ländern verwendet werden. So nutzen beispielsweise Premiere in Deutschland, Digital+ in Spanien, Cyfrowy Polsat in Polen und Echostar in den USA das System Nagravision.[211] Wird Crack-Software auf einem Server in einem beliebigen Land bereitgestellt, ist sie weltweit abrufbar. In speziellen Internetforen tauschen sich Hacker aus der ganzen Welt über ihre neuesten Erkenntnisse und Methoden aus. Die Geschäftspraktiken der Piraten ändern sich dabei permanent, um ihren Jägern immer einen Schritt voraus zu sein.[212] Eine effektive Bekämpfung lässt sich daher nur durch einen Zusammenschluss aller Betroffener erreichen, bei dem ein weitreichender Informationsaustausch über die neuesten Erkenntnisse und Abwehrmethoden stattfindet. Die internationale Kooperation wird auch dadurch gerechtfertigt, dass ein erfolgreicher Schlag gegen Piraten oft mehreren Firmen in verschiedenen Ländern zu Gute kommt.[213] Wird beispielsweise in einem Land ein Ring von Dealern ausgehoben, der mit Smartcards mehrerer internationaler Pay-TV-Sender und Decoderboxen verschiedener Hersteller handelt, profitieren hiervon alle betroffenen Sender und Boxenhersteller in den jeweiligen Ländern. Wird ein Hacker oder eine Gruppe von Hackern ausfindig gemacht, profitieren neben dem Hersteller der Verschlüsselung auch alle Sender, die diese Verschlüsselung nutzen. Daher sollte ein Pay-TV-Anbieter nicht auf ein Engagement in diesen Organisationen verzichten in der Hoffnung, selbst als free-rider von den positiven externen Effekten der Bekämpfungserfolge zu profitieren. Darüber hinaus werden Erfolge gegen die Piraterie wahrscheinlicher, je mehr know-how und finanzielle Mittel zur Verfügung stehen. Je größer die Organisation, desto größer wird auch ihr Einfluss, der für intensive Lobbyarbeit bei Behörden und Politikern genutzt werden kann.

Problematisch ist auch hier, dass sich die Auswirkungen der erzielten Erfolge der Organisationen oder der betriebsinternen Maßnahmen für das eigene Unternehmen nicht immer konkret quantifizieren lassen. Welchen Schaden ein gefasster Hacker einem bestimmten Pay-TV-Sender in Zukunft zugefügt hätte, lässt sich ebenso wenig beziffern wie die Höhe einer Schadensreduktion durch ein neu eingeführtes Gesetz. Den anfallenden Kosten, die sich hingegen recht exakt ermitteln lassen können, z.B. durch die Ermittlung der aufgewendeten

---

[210] 260,40€ x 27

[211] Schubert Juliane, 2004c

[212] o.V., 2003(8)

[213] Vgl. Lievaart, 2001, S. 3.

Arbeitsstunden für ein Projekt oder ein Engagement, kann als Nutzen daher auch im Nachhinein nur ein Schätzwert gegenübergestellt werden. Grundsätzlich ist jedoch auch hier die optimale Kosten-Nutzen-Relation anzustreben, dies bedeutet, dass die Kosten für die Teilnahme an Konferenzen, Informationsaufbereitung und -weitergabe etc. nur bis zu dem Punkt ausgeweitet werden sollten, an dem der zusätzliche bewertete Nutzen aus den erhaltenen Informationen und Bekämpfungserfolgen die zusätzlichen Kosten für ein weiteres Engagement nicht mehr übertrifft.

3.6. Juristische Maßnahmen gegen die Pay-TV-Piraterie

Das Vorgehen gegen die Pay-TV-Piraterie muss zusätzlich durch rechtliche Maßnahmen flankiert werden. Sowohl Hacker als auch Dealer von Piraterie-Technik und Schwarzseher verstoßen gegen eine Reihe von Gesetzen, die hohe Strafen nach sich ziehen können. Die betroffenen Unternehmen, wie Pay-TV-Anbieter oder Hersteller von Codier- und Decodertechnik, ergreifen Anstrengungen, Pay-TV-Piraten ausfindig zu machen und ihre Vergehen juristisch zu ahnden.

3.6.1. Gesetzliche Grundlagen

Als gesetzliche Grundlagen für das juristische Vorgehen gegen Pay-TV-Piraterie kommen insbesondere folgende Gesetze in Betracht:

Hersteller von Piraterie-Equipment können verstoßen gegen

§ 27 Strafgesetzbuch (StGB): Beihilfe[214],

§ 202a StGB: Ausspähen von Daten[215],

§ 269 StGB: Fälschung beweiserheblicher Daten[216],

§ 270 StGB[217]: Täuschung im Rechtsverkehr bei Datenverarbeitung,

§ 303a StGB: Datenveränderung[218],

§ 17 Abs. 2 Gesetz gegen den unlauteren Wettbewerb (UWG): Verrat von Geschäfts- und Betriebsgeheimnissen[219],

§ 106 Urheberrechtsgesetz (UrhG)[220]: Unerlaubte Verwertung urheberrechtlich geschützter Werke,

§ 108 UrhG: Unerlaubte Eingriffe in verwandte Schutzrechte[221],

§ 95a UrhG: Schutz technischer Maßnahmen in Verbindung mit

---

[214] o.V., o.J.(19).

[215] Vgl. Goedecke, Hofmeir, 2003d.

[216] ebenda

[217] Vgl. o.V., 2003(1).

[218] ebenda

[219] Vgl. Goedecke, Hofmeir, 2003d.

[220] o.V., o.J.(19)

[221] Vgl. o.V., 2003(1).

§ 108b UrhG: Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen und

§ 111a UrhG: Bußgeldvorschriften,

§§ 3, 4 Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (ZKDSG): Unerlaubte Herstellung einer Umgehungsvorrichtung[222].

Dealer von Piraterie-Equipment können beim Vertrieb verstoßen gegen

§ 111 StGB: Öffentliche Aufforderung zu Straftaten bei Bewerbung von Umgehungsvorrichtungen[223],

§ 261 StGB: Verschleierung unrechtmäßig erlangter Vermögenswerte (Geldwäsche) [224],

§ 95a UrhG: Schutz technischer Maßnahmen in Verbindung mit

§ 108b UrhG: Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen und

§ 111a UrhG: Bußgeldvorschriften,

§ 3 ZKDSG: Verbot von gewerbsmäßigen Eingriffen zur Umgehung von Zugangskontrolldiensten. § 3 Nr. 3 ZKDSG verbietet jegliche Absatzförderung von Umgehungsvorrichtungen[225].

Nutzer von Piraterie-Equipment können verletzen

§ 261 StGB: Verschleierung unrechtmäßig erlangter Vermögenswerte (Geldwäsche) [226],

§ 263a StGB: Computerbetrug[227],

§ 265a StGB: Erschleichen von Leistungen[228],

§ 269 StGB: Fälschung beweiserheblicher Daten[229],

§ 270 StGB[230]: Täuschung im Rechtsverkehr bei Datenverarbeitung,

§ 95a UrhG: Schutz technischer Maßnahmen in Verbindung mit

§ 111a UrhG: Bußgeldvorschriften.

Das Strafmaß kann je nach Straftat bis zu fünf Jahre Freiheitsentzug betragen. Jeder Verstoß zieht Unterlassungs- und Schadenersatzansprüche nach sich.[231] Zu beachten ist, dass die hier aufgelisteten Gesetzesparagraphen die denkba-

---

[222] Goedecke, Hofmeir, 2003d

[223] ebenda

[224] ebenda

[225] Goedecke, Hofmeir, 2003d

[226] o.V., 2003(1), sowie Goedecke, Hofmeir, 2003d

[227] ebenda

[228] ebenda

[229] ebenda

[230] o.V., 2003(1)

[231] Goedecke, Hofmeir, 2003d

ren sind, gegen die im Falle der Pay-TV-Piraterie verstoßen werden kann. Welche von ihnen tatsächlich zur Anwendung kommen, ist einzelfallabhängig.[232]

Da es den Pay-TV-Anbietern nur in den wenigsten Fällen gelingt, die Schwarzseher ausfindig zu machen, ist es wesentlich effektiver, die Verfolgung auf die Hersteller oder Fälscher illegaler Smartcards und weiteren Piraterie-Equipments sowie deren Vertreiber zu konzentrieren. Der Hersteller macht sich der Beihilfe zu den Straftaten des Schwarznutzers nach § 27 StGB schuldig. Allerdings setzt die Beihilfe stets die Begehung der Haupttat voraus, so dass der Pay-TV-Sender beweisen muss, dass z.B. eine Piratenkarte tatsächlich von einem Schwarzseher angewendet wurde. Derjenige, der lese- und kopiergeschützte Informationen von einer Smartcard ausliest, kann sich nach § 202a StGB des Ausspähens von Daten schuldig machen. Selbst wenn die gespeicherten Daten nicht besonders geschützt sind, greift der Paragraph, da die Smartcard selbst einen Zugangsschutz in bezug auf die angebotenen Leistungen, hier die Pay-TV-Sendungen, darstellt.

Computer- und Betriebsprogramme, die den Betrieb von Decodern steuern, sind Daten bzw. Vorrichtungen zur Entschlüsselung eines Sendesignals, die als Geschäfts- und Betriebsgeheimnisse im Sinne des § 17 Abs. 1 UWG gelten. Diese Eigenschaft bleibt auch bestehen, wenn diese Daten geknackt werden und innerhalb der Hacker-Szene verbreitet werden. Sofern diese Daten jedoch z.B. im Internet veröffentlicht und damit für jedermann zugänglich werden, ist es fraglich, ob die Geheimniseigenschaft weiterhin gegeben ist. Die Herstellung der Piratenkarten verstößt gegen § 17 Abs. 2 Nr. 1 UWG, die Nutzung und der Vertrieb gegen § 17 Abs. 2 Nr. 2 UWG, da durch den Verkauf ein Wettbewerbsverhältnis zum Pay-TV-Anbieter hergestellt wird, zumindest jedoch die Absicht besteht, dem Sender einen Schaden zuzufügen.[233] Das Strafmaß liegt bei bis zu drei Jahren Freiheitsstrafe oder Geldstrafe, in besonders schweren Fällen drohen sogar bis zu fünf Jahre Freiheitsstrafe. Wird mit gestohlenen Smartcards oder Decoderboxen gehandelt, kommt der Straftatbestand der Hehlerei nach § 259 StGB hinzu.

§ 95a Abs. 1 UrhG verbietet ohne Zustimmung des Rechtsinhabers die Umgehung wirksamer technischer Maßnahmen, die dem Schutz urheberrechtlich geschützter Werke dienen. Zu derartigen technischen Maßnahmen gehören auch Zugangskontrollen und Schutzmechanismen wie Verschlüsselungen. § 95a Abs. 3 UrhG untersagt „die Herstellung, die Einfuhr, die Verbreitung, [den] Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung und [den] gewerblichen Zwecken dienende[n] Besitz von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen“, die die Umgehung der technischen Schutzmaßnahmen ermöglichen oder erleichtern. Unter den Begriff Verbreitung fällt auch die Weitergabe derartiger Vorrichtungen auf unkörperlichem Wege, beispielsweise über das Internet.[234] Dienstlei-

---

[232] Bahr, o.J.

[233] o.V., o.J.(19)

[234] Bechtold, 2004, S. 37

stungen im Sinne dieses Gesetzes sind auch Anleitungen zur Umgehung. Danach kann die Verbreitung von Umgehungsanleitungen im Internet oder in der Fach-Presse nach § 95a Abs. 3 UrhG verboten sein.[235] Wird eine Umgehungsvorrichtung zu gewerblichen Zwecken hergestellt, eingeführt, verbreitet, verkauft oder vermietet, kann dies nach § 108b Abs. 2 UrhG mit Geldstrafe oder einer Freiheitsstrafe bis zu einem Jahr geahndet werden. Sofern dieser Paragraph nicht greift, kann eine Ordnungswidrigkeit nach § 111a Abs.1 Nr.1 UrhG vorliegen,[236] demzufolge eine Geldbuße bis zu 50.000,- Euro gegen denjenigen verhängt werden kann, der entgegen § 95a Abs. 3 UrhG „eine Vorrichtung, ein Erzeugnis oder einen Bestandteil verkauft, vermietet oder über den Kreis der mit dem Täter persönlich verbundenen Personen hinaus verbreitet oder zu gewerblichen Zwecken eine Vorrichtung, ein Erzeugnis oder einen Bestandteil besitzt, für deren Verkauf oder Vermietung wirbt oder eine Dienstleistung erbringt.“ Der private Besitz oder Gebrauch der Umgehungsvorrichtungen ist zwar nach § 95a UrhG verboten, steht jedoch nicht unter Strafe. Dennoch können zivilrechtliche Schadensersatz-, Unterlassungs- und Vernichtungsansprüche geltend gemacht werden.[237]

Einzelfallabhängig ist die Anwendbarkeit der Paragraphen 106 und 108 des Urheberrechtsgesetzes. § 106 UrhG kann nur angewendet werden, wenn Originalsoftware des Pay-TV-Senders unter Verletzung der Lizenzbestimmungen vervielfältigt wird, § 108 Abs. 1 Nr. 8 UrhG nur, wenn die Daten auf der Smartcard als Datenbank oder Teil einer Datenbank gemäß § 87b UrhG gelten.[238] Beide Paragraphen sehen eine Geldstrafe oder eine Freiheitsstrafe von bis zu drei Jahren vor.

Während § 95a UrhG nur im Falle urheberrechtlich geschützter Werke zum Tragen kommt, findet das Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (ZKDSG) unabhängig von der Art des geschützten Inhalts Anwendung.[239] Nach diesem sind bestimmte Verwendungsformen von Umgehungseinrichtungen verboten.[240] Umgehungsvorrichtungen im Sinne des Gesetzes sind „technische Verfahren oder Vorrichtungen, die dazu bestimmt oder entsprechend angepasst sind, die unerlaubte Nutzung eines zugangskontrollierten Dienstes zu ermöglichen“. Darunter fallen Computerprogramme zur Manipulation von Decoderboxen sowie Plagiate und Nachbauten von Zugangskontrollsystemen wie manipulierte oder nachgemachte Smart-

---

[235] ebenda, S. 38

[236] ebenda, S. 43

[237] ebenda, S. 26

[238] o.V., o.J.(19)

[239] Vgl. Bechthold, 2004, S. 50. Der Ursprung des ZKDSG liegt tatsächlich in der Piraterie-Problematik des verschlüsselten Pay-TV. Es wird daher auch als „Lex Premiere“ bezeichnet. Siehe hierzu z.B.: Bär, Hoffmann, 2002, S. 654ff. und Bechtold, 2004, S. 46.

[240] o.V., o.J.(19)

cards.[241] § 3 Nr. 1 ZKDSG verbietet die Herstellung, Einfuhr und Verbreitung zu gewerbsmäßigen Zwecken, § 3 Nr. 2 den Besitz, die technische Einrichtung, Wartung und Austausch von Umgehungsvorrichtungen zu gewerbsmäßigen Zwecken. § 3 Nr. 3 untersagt die Absatzförderung dieser Vorrichtungen, auch bei nicht gewerbsmäßigem Handeln, sofern damit kommerzieller Absatz in Handel, Gewerbe, Handwerk oder freien Berufen gefördert wird.[242] Gewerbsmäßige Zwecke sind dann zu unterstellen, wenn die Tätigkeit nachhaltig ist und der Erzielung von Einnahmen dient. Nicht notwendig ist dabei eine Gewinnerzielungsabsicht.[243] Auch hier fällt unter den Begriff Verbreitung auch die unkörperliche Distribution, insbesondere über das Internet.[244] Verstöße gegen § 3 Nr. 1 ZKDSG werden mit einer Geldstrafe oder Freiheitsstrafe bis zu einem Jahr geahndet, Verstöße gegen § 3 Nr. 2 ZKDSG stellen eine Ordnungswidrigkeit dar und werden mit einer Geldbuße bis zu 50.000 Euro belegt. § 3 ZKDSG ist ein Schutzgesetz nach § 823 Abs. 2 BGB. Demnach haben Anbieter von zugangskontrollierten Diensten im Rahmen des Schadensersatzes bzw. nach den Rechtsgrundsätzen der ungerechtfertigten Bereicherung Anspruch auf die Gewinne, die durch die Umgehungsvorrichtungen erzielt wurden. Außerdem können die Anbieter gegenüber den Händlern Unterlassungsansprüche nach § 8 in Verbindung mit § 3 UWG sowie nach § 1004 und § 823 Abs. 2 BGB in Verbindung mit Schutzgesetzverletzungen geltend machen.[245] Zu beachten ist, daß der private Besitz von Umgehungsvorrichtungen wie nachgebauten Decoderboxen nicht verboten ist.[246]

3.6.2. Juristisches Vorgehen gegen die Pay-TV-Piraten

Im Gegensatz zu den Anfangsjahren des Pay-TV, in denen die Anbieter juristische Maßnahmen gegen die Piraten scheuten, um die Öffentlichkeit nicht auf die Verletzbarkeit der Schutzvorrichtungen aufmerksam zu machen[247], gehen sie heute gegen Schwarzseher, Hersteller und Händler von Piraterie-Equipment mit einstweiligen Verfügungen, Gerichtsurteilen und Razzien bei Händlern und in Privathaushalten vor.[248] Im Oktober 2002 erwirkte die Firma SCM Microsystems, Hersteller von Smartcard Reader-Technologie und Conditional-Access-Modulen[249], eine einstweilige Verfügung gegen die Herstellung und den Vertrieb des sogenannten „Magic Moduls“. Das Magic Modul wurde offiziell zwar nur als gewöhnliches Smartcard-Lesemodul beworben, es eignete sich jedoch auch zur

---

[241] ebenda

[242] Bär, Hoffmann, 2002, S. 655. Die Förderung eines privat tätigen Dritten wird damit nicht erfasst.

[243] o.V., o.J.(19)

[244] Bechtold, 2004, S. 46

[245] Vgl. o.V., o.J.(19).

[246] Bechtold, 2004, S. 47

[247] o.V., 2003(3), S. 21

[248] Goedecke, Hofmeir, 2003c, S. 24

[249] o.V., o.J.(22)

Umgehung der Zugangskontrolle für Pay-TV. In zahlreichen Internet-Foren wurde das Modul zur Entschlüsselung von Pay-TV empfohlen. Die dazu benötigte Software wie z.B. „Pentacrypt“ konnte aus dem Internet, insbesondere von ausländischen Webseiten, heruntergeladen werden. Das Gericht bestätigte daher einen Verstoß gegen das ZKDSG und erließ eine einstweilige Verfügung gegen zwei Großhändler des Magic Moduls.[250] Auch gegen die Abwandlungsformen des Magic Moduls wie KidCam, MatrixCam, UniversalCam, JokerCam und andere geht SCM mit Abmahnungen und Schadensersatzklagen vor.[251] Hinzu kommt, dass bei der Aufspielung der Software des Verschlüsselungssystems auf die bei Erwerb blanken Module nach Meinung der Verschlüsselungsanbieter Patente, Urheberrechte und Lizenzbestimmungen verletzt werden. Allein SCM Microsystems ist zur Herstellung der Module mit der entsprechenden Verschlüsselungssoftware berechtigt.[252] In seinem Beschluss vom 05. Juni 2003 bestätigte das Oberlandesgericht Frankfurt a.M. das Verbot des Bewerbens und des Vertriebs von Magic Modulen aufgrund der Verletzung von § 1 UWG i. V m. §§ 2 Nr. 3 und 3 ZKDSG. Das Magic Modul sei als Umgehungsvorrichtung im Sinne von § 2 Nr. 3 ZKDSG anzusehen. Ausschlaggebend für die Einschätzung als Umgehungsvorrichtung ist nach Auffassung des Gerichts nicht der vom Hersteller angegebene Verwendungszweck, sondern die Zweckbestimmung des Geräts, die der verständige Durchschnittsnutzer annimmt. Auf diese Weise soll verhindert werden, dass das Verbot durch Scheinhinweise umgangen werden kann. Neben dem Verstoß gegen das ZKDSG wurde noch ein Verstoß gegen § 1 UWG alter Fassung (Verstoß gegen die guten Sitten zu Zwecken des Wettbewerbs) festgestellt, da das ZKDSG die Hersteller legaler Entschlüsselungsvorrichtungen vor illegalem Wettbewerb schützen soll.[253]

Auch Premiere geht verstärkt gegen Händler und Nutzer von Piraterie-Technik vor. Sogar Privatpersonen, die bei ebay Schreib-/Lesegeräte für Smartcards oder leere Smartcards anbieten, werden mit mehreren hundert Euro abgemahnt. Die Adressen der Anbieter erhalten die Premiere-Anwälte dabei direkt von ebay. Im Jahr 2003 untersagte das Landgericht Hamburg auf Antrag von Premiere die Verbreitung und Bewerbung von Blanko-Smartcards und der entsprechenden Programmiergeräte, sofern davon auszugehen ist, dass die beworbenen Geräte durch die Nutzer mit hoher Wahrscheinlichkeit zur unerlaubten Nutzung von Abo-TV verwendet werden. Im konkreten Fall erließ das Landgericht eine einstweilige Verfügung gegen einen der größten Händler von Blanko-Smartcards und Programmiergeräten in Deutschland. Der Händler bewarb diese Produkte auf Internetseiten zusammen mit Anleitungen und Software zum Hacken von Pay-TV. Missachtet der Händler die Anordnung des Gerichts, droht ihm ein Ordnungsgeld bis zu 250.000 Euro oder Ordnungshaft zwischen sechs Monaten und zwei Jahren. Premiere sieht in diesem Urteil einen wichtigen Er-

---

[250] Hofmeir, 2003a, S. 17

[251] Goedecke, Hofmeir, 2003b, S. 37

[252] o.V., 2002(5) sowie o.V., 2002(8)

[253] o.V., 2003(6)

folg im Kampf gegen die Karten-Dealer, da die Verbreitung der Blanko-Smartcards und dadurch auch der Handel mit gefälschten Smartcards durch die Verfügung erheblich erschwert wird.[254]

Angriffsziel von deutschen Hackern und Schwarzsehern ist jedoch nicht nur das deutsche Pay-TV-Angebot, auch ausländische Programme, die in Deutschland empfangen werden können, wie z.B. verschlüsselte Kanäle aus der Schweiz und Österreich mit ihrem deutschsprachigen Programm oder italienische und französische Kanäle, die Filme in englischer Originalsprache ausstrahlen, sind für sie attraktiv.[255] Da Fernsehsignale bei der Aussendung nicht einfach räumlich begrenzt werden können, strahlen sie auch über Ländergrenzen hinweg in das Ausland. Auch dort können die Sendungen mittels eines Decoders empfangen werden. Allerdings bezahlen die ausländischen Empfänger in der Regel nicht an den Pay-TV-Sender, sondern nur für die Beschaffung der Decoder und Smartcards an Grauimporteure oder solche Anbieter, die den Code entschlüsselt haben. Bevor ein Pay-TV-Anbieter gegen solcherlei Machenschaften vorgehen kann, muss er jedoch eine gültige Sendelizenz für das betreffende Land vorweisen können.[256] Mit welchen Problemen die Bekämpfung der länderübergreifenden Piraterie-Bekämpfung verbunden sein kann, zeigt folgendes Beispiel: Der französische Pay-TV-Sender Canal+ besaß keine Genehmigung für eine Ausstrahlung in der Schweiz. Als in der französischsprachigen Schweiz Decoder, mit denen sich Canal+ entschlüsseln ließ, in hoher Stückzahl vertrieben wurden, verklagte Canal+ den Hersteller und Vertreiber der Geräte. Vor Gericht verlor der Sender: Da Canal+ nicht autorisiert sei, in der Schweiz kommerziell tätig zu sein, könne der Sender folglich auch keine Verletzung seiner wirtschaftlichen Interessen geltend machen.[257]

3.6.3. Kosten-Nutzen-Abwägung der rechtlichen Maßnahmen

Juristische Maßnahmen gegen Pay-TV-Piraten sind unerlässlich. Um Gesetzesverstöße zu ahnden, müssen diese zunächst aufgedeckt werden. Öffentliche Behörden wie Polizei und Staatsanwaltschaft sind oft überfordert und überlastet, so dass die Unterstützung durch die betroffenen Unternehmen notwendig wird. Auch wenn Premiere-Chef Kofler droht, dass sein Unternehmen ausnahmslos gegen jeden Hacker, Dealer oder Schwarzseher vorgehen wird[258], sollten die durchgeführten Ermittlungen nicht das Ziel haben, vereinzelt Schwarzseher ausfindig zu machen, um diese vor Gericht zu stellen. Kosten und Nutzen stünden in keinem vernünftigen Verhältnis. Das Ziel sollte statt dessen sein, das Übel an der Wurzel zu packen und vor allem gegen organisierte Piraterie-Aktivitäten vorzugehen. Insbesondere Hacker als die Quellen und Dealerringe als die Distributoren der Piraterie-Technik sollten im Mittelpunkt der Ermittlun-

---

[254] Goedecke, Hofmeir, 2003d sowie o.V., 2003(7)

[255] Hankmann, Sprotte, 2004c, S. 86

[256] Vgl. Karepin, 1993, S. 61.

[257] Große Peclum, 1991, S. 81

[258] o.V., 2002(7)

gen stehen. Schwarzseher werden automatisch mitbekämpft, indem ihnen die Bezugsquellen genommen werden. Durch die konsequente Verfolgung und vor allem durch publik gemachte Ermittlungserfolge wird zum einen die Glaubwürdigkeit in der Öffentlichkeit hergestellt, dass der Ausschluss von Schwarzsehern den Pay-TV-Sendern ein ernstes Anliegen ist, zum anderen dienen sie der Abschreckung, indem der Öffentlichkeit vermittelt wird, dass Schwarzsehen kein Kavaliersdelikt ist und ernsthafte Konsequenzen nach sich zieht. Schulungsmaßnahmen durch die Pay-TV-Anbieter, mit denen Polizei und Rechtsanwälte auf den neuesten Stand gebracht werden, sind ebenfalls notwendig, da nur mit Hilfe der Exekutive und der Judikative rechtliche Maßnahmen durchgesetzt werden können.

Zu bedenken ist jedoch, dass auch der Weg über die Bekämpfung der Hacker und Dealer sehr schwierig und nicht unbedingt von Erfolg gekrönt ist. In den USA stellte beispielsweise der Pay-TV-Sender DirecTV fest, dass allein die Bekämpfung der Dealer nicht den gewünschten Erfolg brachte und begann deswegen, Jagd auf die Schwarzseher zu machen. Diese wurden mit Hilfe der Kundenlisten der Dealer ausfindig gemacht. Daraufhin verschickte der Sender über 170.000 Abmahnungen und strengte mehr als 24.000 Klagen gegen sie an. Die Bemühungen wurden jedoch bisher nicht belohnt, da ein US-Berufungsgericht den bloßen Besitz von Umgehungstechnik als Klagegrund für nicht ausreichend erachtete. Zusätzlich sei auch der Nachweis der missbräuchlichen Anwendung zu erbringen.[259]

Dem Nutzen der juristischen Maßnahmen stehen vor allem Kosten für die permanenten Ermittlungsmaßnahmen durch eigene Mitarbeiter, für juristische Aktivitäten wie z.B. Abmahnungen, die durch eigenes Personal oder externe Rechtsanwälte übernommen werden, und im Falle einer gerichtlichen Auseinandersetzung die Verfahrenskosten, soweit sie nicht vom Gegner getragen werden, gegenüber. Hinzu kommen die Kosten für die Schulungsmaßnahmen bei den Behörden und Anwälten:

$K_{JM} = K_E + K_{JV} + K_{SM}$,

mit

K_{JM}: Kosten für juristische Maßnahmen

K_E: Kosten für Ermittlungen

K_{JV}: Kosten für juristische Verfolgung

K_{SM}: Kosten für Schulungsmaßnahmen für Behörden und Anwälte

Die Kosten für die Ermittlungsarbeit bestehen im wesentlichen aus dem Zeitaufwand, den die ermittelnden Mitarbeiter pro Fall benötigen:

$K_E: k_p/t * M * T$,

mit

T: Gesamtdauer der Beschäftigung mit einem Fall

---

[259] o.V., 2004(6).

Die Kosten der juristischen Verfolgung setzen sich aus dem Zeitaufwand der beteiligten eigenen Mitarbeiter, den Kosten für beauftragte externe Anwälte und den Gerichts- und sonstigen Prozesskosten zusammen:

K_{JV}: $k_p/t * M * T + K_A + K_P$

mit

K_A: Kosten für externe Anwälte für einen Fall

K_P: Gerichts- und sonstige Prozesskosten eines Falles

Die für die durchgeführten Schulungsmaßnahmen entstehenden Kosten bestehen ebenfalls vor allem aus dem Zeitaufwand für die Vorbereitung und Durchführung der Schulungen:

$K_{SM} = k_p/t * M * T$,

mit

T: gesamter Zeitaufwand für Vorbereitung und Durchführung der Schulungen

Sämtliche Kosten sollten in einem angemessenen Verhältnis zu den Erfolgen stehen. Doch gerade der Erfolg der Maßnahmen ist nicht vorauszusagen. Es ist nicht sicher, ob Ermittlungen tatsächlich zu Pay-TV-Piraten führen, ob ihnen juristisches Fehlverhalten nachgewiesen werden kann, welches für polizeiliche und gerichtliche Maßnahmen ausreicht, oder wie ein Gerichtsverfahren ausgehen wird. Hier kann nur mit Wahrscheinlichkeiten und Erwartungswerten gerechnet werden. Beispielsweise sollte der Erwartungswert für die Höhe des Schadenersatzes, den das Unternehmen erhält, höher sein, als die erwarteten anfallenden Kosten für Ermittlungen, Anwälte und Gerichtsverfahren. Der Erwartungswert resultiert dabei aus der Wahrscheinlichkeit einer Verurteilung des Täters und der Höhe des erwarteten Schadenersatzes. In die Berechnung sollte auch einbezogen werden, wie hoch der Schaden wäre, der durch die Verurteilung eines Pay-TV-Piraten in Zukunft vermieden wird. Verursacht beispielsweise ein Händler illegaler Smartcards dem Pay-TV-Anbieter durch den Verkauf der Karten jährlich einen Schaden von 100.000,- Euro pro Jahr, bedeutet eine Verurteilung des Täters für den Sender in Zukunft eine jährliche Schadensminimierung um diese 100.000,- Euro. Hier ist es sinnvoll, insbesondere gegen Hacker und Händler vorzugehen. Ihnen können im Falle eines Verfahrens mit hoher Wahrscheinlichkeit vorsätzliche Verstöße gegen eine Reihe von Gesetzen nachgewiesen werden, die mit hohen Strafen belegt sind. Gleichzeitig ist der abgewendete finanzielle Schaden durch sie in der Regel deutlich höher als der Schaden durch einzelne Schwarzseher. Zusätzlich werden durch die abschreckende Wirkung von Verfolgung und Verurteilungen Zuschauer vom Schwarzsehen und Hacker und Dealer von ihren illegalen Machenschaften abgehalten, da sie ähnliche Konsequenzen fürchten. Dies vermeidet ebenfalls Einnahmeausfälle.

$N_{JM} = E_{SE} + VS$,

mit

N_{JM} : Nutzen der juristischen Maßnahmen

E_{SE} : zugesprochener Schadensersatz

VS : verhinderter Schaden durch abgewendete Einnahmeausfälle

Der verhinderte Schaden setzt sich aus den abgewendeten Einnahmeausfällen zum einen durch erfolgreich bekämpfte Piraterie, zum anderen durch die abschreckende Wirkung bei Piraten zusammen:

$VS = E_{VPA} + E_{Ab}$,

mit

E_{VPA}: verhinderte Einnahmeausfälle durch vermiedene Piratenaktivitäten

E_{Ab}: verhinderte Einnahmeausfälle durch abschreckende Wirkung bei Zuschauern, Hackern und Dealern.

Auch bei der juristischen Verfolgung sollte sich ein Pay-TV-Sender ökonomisch rational verhalten und darauf achten, dass keine höheren Kosten entstehen als Nutzen aus den Maßnahmen gezogen werden kann. Daher sollte immer gelten:

$N_{JM} > K_{JM}$.

Während sich die Kosten für einzelne Fälle nach Abschluss nachvollziehen lassen, kann der Nutzen in Form von Einnahmen nur teilweise beziffert werden. Zusätzlich zu erhaltenen Schadensersatzzahlungen müssen die zukünftig verhinderten Einnahmeausfälle berücksichtigt werden, diese können jedoch nur geschätzt werden.

3.7. Kosten-Nutzen-Bewertung der Bekämpfung der Pay-TV-Piraterie

Das Ausmaß der Abwehrmaßnahmen gegen die Schwarzseher muss auf dem Prinzip der Wirtschaftlichkeit beruhen.[260] Daher sollten sämtliche Bekämpfungsmaßnahmen einen höheren Nutzen stiften als sie Kosten verursachen:

$N_{SB} > K_{SB}$,

mit

N_{SB}: Nutzen der Schwarzseherbekämpfung

K_{SB}: Kosten der Schwarzseherbekämpfung

Premiere schätzte z.B. den Schaden, der dem Sender durch die Schwarzseher entsteht, im Jahr 2003 auf 100 Millionen Euro jährlich[261]. Die Bekämpfungsmaßnahmen gegen die Schwarzseher sollten Premiere daher keine Kosten verursachen, die 100 Millionen Euro pro Jahr überschreiten. Dies setzt voraus, dass die angewendeten Maßnahmen das Schwarzsehen vollständig beseitigen. Wird

[260] Vgl. Tetzner, 1991, S. 21.

[261] Pötzsch, 2003

keine vollständige Beseitigung angestrebt oder erreicht werden können, sollte dennoch jeder eingesetzte Betrag zur Schwarzseherbekämpfung durch den Betrag der dadurch erreichten Schadensreduktion übertroffen werden. Wird z.B. ein Betrag von 50 Millionen Euro eingesetzt, sollte der Schaden dadurch um mehr als 50 Millionen Euro reduziert werden.

Problematisch bei der Kosten-Nutzen-Bewertung ist, dass viele Kosten- und Nutzen- bzw. Einnahmewerte nur geschätzt werden können. Zusätzlich dient die Kosten-Nutzen-Analyse als Entscheidungsinstrument für zukünftige Handlungen, so dass auch die eingesetzten Werte zukunftsgerichtet und damit unsicher sind. Daher müssen für die Entscheidungen Erwartungswerte auf der Grundlage der geschätzten und unsicheren Daten herangezogen werden. Ob eine Bekämpfungsmaßnahme tatsächlich einen kostenüberlegenen Nutzen gestiftet hat, kann auch im Nachhinein nur bedingt festgestellt werden, da auch dann noch Schätzwerte herangezogen werden müssen. Beispielsweise lässt sich nicht nachprüfen, wie viele Zuschauer tatsächlich aufgrund einer vorübergehend nicht überwindbaren Verschlüsselung zu Abonnenten werden.

3.8. Exkurs: DirecTV

DirecTV ist in den USA der marktführende Anbieter von Pay-TV über Satellit.[262] Auch dieser Sender hat mit dem Schwarzseher-Problem zu kämpfen und geht seit Juli 2001 offensiv gegen die Pay-TV-Piraten vor. Hierfür verfügt auch DirecTV über eine eigene Abteilung, die Abteilung für Signal-Integrität.[263] An Tausende Haushalte verschickte das Unternehmen damals Abmahnungen mit der Aufforderung, schriftlich zu versichern, zukünftig keine Schwarzseh-Aktivitäten mehr vorzunehmen.[264] Nachdem die Bekämpfungs-Bemühungen jahrelang einem Katz-und-Maus-Spiel glichen, gelang dem Sender Anfang 2001 ein bemerkenswerter Coup: An Millionen Pay-TV-Receiver wurde ein Signal ausgestrahlt, welches durch Hacker manipulierte Fernsehkarten unbrauchbar machte, die einen kostenlosen Empfang des Programms am heimischen PC ermöglicht hatten. Von dieser Attacke waren rund 200.000 Schwarzseher betroffen, ein Ausmaß, welches die Pay-TV-Piraten von einem „Schwarzen Sonntag“ sprechen ließ. Auch die Abschreckungswirkung dieser Aktion wurde in Hacker-Kreisen anerkannt, da Karten im Wert von 350 Dollar pro Stück mit einem Mal wertlos waren.[265]

DirecTV lässt außerdem Internet-Seiten mit Inhalten für den illegalen Pay-TV-Zugang sperren und verlinkt sie statt dessen zu einer eigenen Seite[266], auf der die Piraterie-Bekämpfungsmaßnahmen des Unternehmens aufgeführt werden. Gegenwärtig wird auf der Seite bekannt gegeben, dass DirecTV bereits gegen

---

[262] Buschendorf, 2005b

[263] Peeck, 2001

[264] Adamcewski, 2002

[265] o.V., 2001a

[266] Umgeleitete ehemalige Hacker-Seiten sind z.B. http://www.hackhu.com/ oder http://www.dishnethack.com/.

mehr als 24.000 Schwarzseher Gerichtsverfahren geführt hat. Neben der Aufklärung, welche Aktivitäten eines potentiellen Pay-TV-Piraten illegal sind, werden auch die Straf- und Zivilprozesse, die DirecTV gegen die Piraten führt oder geführt hat, und die Namen der Beklagten auf dieser Seite bekannt gegeben.[267]

In den USA verstoßen Herstellung, Montage, Modifizierung, Import, Export, Verkauf oder Distribution von Geräten zur unerlaubten Entschlüsselung gegen den Paragraphen 605 Abs. (e) (4) (47 U.S.C. § 605, Unauthorized Publication or Use of Communications). Dieser sieht pro Vergehen eine Geldstrafe von bis zu 500.000 Dollar oder eine Gefängnisstrafe von bis zu fünf Jahren oder beides vor. Zusätzlich steht nach dem Telecommunication Act von 1996 der Kauf von Geräten in der Absicht der Hintergehung von Kabel- und Satelliten-Service-Anbietern unter Strafe, die bis zu 10.000,-$ pro Tat betragen kann.[268] Nach dem „Digital Millennium Copyright Act“ ist es verboten, Geräte oder Services zu vertreiben, die Schutztechnologie urheberrechtlich geschützter Werke umgehen (17 U.S.C. § 1201). Ebenfalls relevant sind 17 U.S.C. §§ 1202, 1203 und 18 U.S.C. §§ 1029 und 2512.[269]

[267] o.V., o.J.(26)

[268] Shepardson, 2002

[269] o.V., o.J.(26)

4. Kosten und Nutzen aus Sicht der Pay-TV-Piraten

Damit das Schwarzsehen für einen Pay-TV-Zuschauer rational ist, muss das Kosten-Nutzen-Verhältnis des Schwarzsehens dem Kosten-Nutzen-Verhältnis eines legalen Zugangs überlegen sein. Zunächst wird nun analysiert, welche Kosten für die legale Nutzung eines Pay-TV-Angebots anfallen. Dem Ergebnis werden dann die Kosten eines illegalen Zugangs gegenüber gestellt.

4.1. Kosten für den Zugang zu Pay-TV

4.1.1. Kosten für den legalen Pay-TV-Zugang

Der Ausschluss durch Verschlüsselung des Fernsehsignals bedeutet für die ehrlichen Kunden, dass sie zusätzlich zu Ihrem Fernsehgerät Entschlüsselungstechnik installieren und verwenden müssen. Dies ist mit Aufwand und Kosten zusätzlich zu den Gebühren verbunden. Zunächst muss ein Decoder angeschafft werden, der die Programme des jeweiligen Pay-TV-Anbieters entschlüsseln kann. Alternativ kann für die meisten Pay-TV-Programme auch ein universeller Decoder mit einer genormten Schnittstelle, dem sogenannten Common Interface (CI), angeschafft werden. An Decoder mit Common Interface können verschiedene CI-Module angeschlossen werden, so dass man mit nur einer Box mehrere Verschlüsselungen decodieren kann.[270] In den Einschubschacht der Schnittstelle wird dann das CI-Modul, auch als Conditional-Access-Modul (CA-Modul oder CAM) bezeichnet, mit der erforderlichen Verschlüsselungsnorm geschoben. Set-Top-Boxen mit der CI-Schnittstelle kosten ab ca. 150,-€.[271] Die Preise für CA-Module betragen zwischen 50,-€ und 200,-€.[272] Einige der Module beherrschen mehrere Verschlüsselungsnormen, z.B. können die Normen AlphaCrypt, Irdeto, Cryptoworks und Conax von einem einzigen Modul entschlüsselt werden. Es muss dann lediglich die Smartcard ausgetauscht werden, um einen anderen Pay-TV-Sender schauen zu können. Zur Zeit wird auch ein Twin Card Modul getestet, welches mittels zweier Kartenleser erstmalig zwei Abokarten gleichzeitig verwalten kann.[273] Sollen mehrere Pay-TV-Programme empfangen werden, die mit Techniken verschlüsseln, die nicht von einem einzigen Decoder oder CI-Modul decodiert werden können, sind mehrere Decoder bzw. CI-Module erforderlich. Diese können entweder käuflich erworben oder nach Hinterlegung einer Kaution gemietet werden. Sollte der Decoder oder das CA-Modul im Handel gekauft werden, ist der damit zusammenhängende Kosten- und Zeitaufwand zu berücksichtigen. Wird per Telefon oder Internet bestellt, fallen auch hier Zeitaufwand und Kosten z.B. für die Telefonverbindung an. Hinzu kommt die Wartezeit, bis die Ware geliefert wird. Zusätzlicher Zeitaufwand ist für die Installation der Geräte notwendig, der vom individuellen technischen Verständnis der Anwender abhängt. Meistens ist die Technik jedoch so konstruiert, dass auch für Laien die Installation problemlos durchführ-

---

[270] Goedecke, Hofmeir, 2003b, S. 36

[271] Vgl. o.V., o.J.(8).

[272] Meyer, Sprotte, 2003a

[273] Schubert, 2004a

bar sein sollte, so dass hierfür in der Regel nur einige Minuten aufgewendet werden müssen.

Die für die jeweiligen Tätigkeiten aufgewendete Zeit ist in Opportunitätskosten zu berechnen und für jeden Einzelnen verschieden. Sie hängt von dem individuellen Stundenlohn ab, der alternativ hätte erworben werden können. Für einen hochbezahlten Manager fallen daher wesentlich höhere Opportunitätskosten an als für einen beschäftigungslosen Rentner.

Nach der Investition in die technischen Voraussetzungen fallen Gebühren für den Empfang der Programme an. Als Kunde eines Abonnement-Fernsehsenders sind regelmäßige, zumeist monatliche Abonnementgebühren zu entrichten, bei Inanspruchnahme von Pay-per-view-Diensten wird das Entgelt pro abgerufenem Film fällig.

4.1.2. Kosten für die Kunden am Beispiel von deutschen Pay-TV-Anbietern

Für den Empfang von Premiere, dem bekanntesten Pay-TV-Angebot in Deutschland[274], ist ein Digital-Receiver notwendig, der als „Premiere geeignet“ gekennzeichnet sein muss.[275] Ein solcher Receiver kann von Premiere zum Preis von 7,50€ im Monat zzgl. einer unverzinsten Kaution in Höhe von 75,-€ gemietet oder käuflich erworben werden.[276] Der Kaufpreis für den Receiver ist abhängig von dem jeweils georderten Abonnement-Paket und beträgt entweder 1,-€, 79,-€ oder 149,-€.[277] Hinzu kommen für die Lieferung des Receivers und der Smartcard eine Versandkostenpauschale von 5,-€ und eine Nachnahmegebühr von 2,-€ (letztere entfällt beim Kauf des Receivers für 1,-€).[278] Im Handel sind Premiere-geeignete Receiver ab 139,-€ (für Satellitenempfang) bzw. 199,-€ (für Kabelempfang) erhältlich.[279] Es ist auch möglich, ein Premiere-geeignetes CI-Modul an einen geeigneten Digitalreceiver anzuschließen.[280] Die Bestellung eines Premiere-Abonnements samt Digitalreceiver kann außer im Handel online auf der Premiere-Homepage oder per Telefon über eine Kundenhotline erfolgen, die für 0,12€ pro Minute zu erreichen ist. Die Ware, bestehend aus der Premiere-Smartcard und dem optionalen Receiver bzw. CI-Modul, wird anschließend innerhalb von 3-5 Werktagen per Post zu der gewünschten Lieferadresse geschickt. Die Installation der Geräte mit Hilfe der Bedienungsanleitung sei nach Angaben auf der Premiere-Homepage „kinderleicht“, sollten jedoch Probleme auftreten, steht dem Kunden eine Technik-Hotline rund um die Uhr

---

[274] o.V., o.J.(17)

[275] o.V., o.J.(11)

[276] o.V., 2004(11)

[277] o.V., o.J.(1)

[278] o.V., 2004(11)

[279] Liebert, 2004

[280] Hagedorn, 2002

zur Verfügung.[281] Diese kostet den Anrufer wiederum 0,12€ pro Minute. In besonders schwierigen Fällen schickt Premiere auch einen sogenannten mobilen Technik-Einsatz zum Kunden. Sollte die Problemursache durch die Premiere-eigene Technik verursacht sein, übernimmt Premiere die Kosten, ansonsten wird dem Kunden der Einsatz in Rechnung gestellt.[282] Bevor Premiere dann freigeschaltet wird, muss durch einen Anruf bei der Hotline die Smartcard noch aktiviert werden.

Die mit dem zeitlichen Aufwand verbundenen Opportunitätskosten entstehen, wie oben bereits erwähnt, individuell für jeden Abonnenten und können daher nicht pauschal in monetären Größen ausgedrückt werden.

Die Abonnementgebühren beginnen bei 5,-€ Monatsgebühr für „Premiere Start“, das teuerste Paket „Premiere Komplett“ kostet bei 12 Monaten Laufzeit 45,-€ im Monat. Wird zusätzlich das Pay-per-view-Angebot „Premiere Direkt“ gewünscht, werden 3,-€ pro Filmabruf fällig.[283] Hinzu kommen die Gebühren für die telefonische Bestellung des gewünschten Films in Höhe von 0,12€ pro Minute oder entsprechende Leitungskosten für die Bestellung per Internet.

Tabelle 1:
Kosten des Premiere-Abonnements

Kosten für das billigste reguläre Premiere-Abonnement	
Receiver (von Premiere)	149,00 €
Versandkostenpauschale	5,00 €
Nachnahmegebühr	2,00 €
Jahresgebühr für "Premiere Start" (12 x 5,-€)	60,00 €
Summe	216,00 €
Kosten für das teuerste reguläre Premiere-Abonnement	
Receiver (von Premiere)	1,00 €
Versandkostenpauschale	5,00 €
Jahresgebühr für "Premiere Komplett" (12 x 45,-€)	540,00 €
Summe	546,00 €

Für einen Neuabonnenten von Premiere ergeben sich also, unter Vernachlässigung der Telefon-Hotline-Gebühren und den Zinsverlusten bei Leistung einer unverzinsten Kaution, bei der Wahl des billigsten und des teuersten Angebotes im ersten Jahr die in Tabelle 1 aufgeführten Kosten. Nach der einmaligen Anschaffung des Receivers fallen in den Folgejahren lediglich die Abonnementge-

[281] o.V., o.J.(11)

[282] Nach Auskunft der Premiere-Kunden-Hotline, Tel.Nr.: 0180/ 511 00 00, vom 14.10.2004.

[283] o.V., 2004(12)

bühren, in diesen Beispielen in Höhe von 60,-€ für das billige bzw. 540,-€ für das teure Angebot an. Hinzu kommen eventuelle Pay-per-view-Gebühren.

Zunehmend bieten auch deutsche Kabelnetzbetreiber Pay-TV-Programme in Form von Abonnements oder Pay-per-view an.[284] Als Beispiele seien hier Kabel Deutschland, Ish und Primacom genannt. Auf das Angebot kann jedoch nur zugegriffen werden, sofern man Kunde des jeweiligen Kabelnetzbetreibers ist. Ish bietet nach einer einmaligen Aktivierungsgebühr in Höhe von 14,95€ und gegen Zahlung einer digitalen Grundgebühr von monatlich 2,-€ einzelne Programme ab 1,-€ pro Monat an, das teuerste Programmpaket kostet 12,50€ im Monat. Einzelne Filme können für 3,-€ bzw. 3,90€ abgerufen werden.[285] Zusätzlich können ausländische Programmpakete für 0,95€ bis 17,95€ pro Monat ge-

Tabelle 2:
Kosten für Ish-Pay-TV

Kosten für das billigste Ish-Pay-TV-Angebot, Laufzeit 1 Jahr	
Receiver von Ish incl. Smartcard	79,00 €
Versandkosten	4,90 €
Aktivierungsgebühr	14,95 €
Digitale Grundgebühr (12 x 2,-€)	24,00 €
Ish "à la carte-Programm" , Preisgruppe 1 (12x1€)	12,00 €
Summe	134,85 €

Kosten für das teuerste deutsche Ish-Pay-TV-Angebot, Laufzeit 1 Jahr	
Receiver von Ish incl. Smartcard	79,00 €
Versandkosten	4,90 €
Aktivierungsgebühr	14,95 €
Digitale Grundgebühr (12 x 2,-€)	24,00 €
Programm-Paket Ish "Premium" (12 x 12,50€)	150,00 €
Summe	272,85 €

ordert werden.[286] Für den Empfang von Ish-Digital-TV ist ein Premiere-geeigneter Receiver notwendig, der bei Ish je nach Vertragslaufzeit zwischen 29,-€ und 149,-€ kostet (79,-€ bei Abschluss eines Einjahresvertrags). In dem Preis ist die Smartcard bereits enthalten. Wird nur die Karte ohne Receiver bestellt, ist eine Bereitstellungsgebühr von 19,90€ zu entrichten. Die Smartcard bleibt dabei Eigentum von Ish. Sie ist nach Vertragsablauf vom Kunden auf eigene Kosten an Ish zurückzuschicken, sofern sie nicht für die Dienste anderer Anbieter genutzt wird.[287] Der Versand des Receivers wird mit 4,90€ berechnet.[288] Ist bereits ein Premiere-Abonnement vorhanden, kann das Pay-Angebot von Ish über die Premiere-Smartcard freigeschaltet werden.[289] Bei einjähriger Laufzeit entstehen

[284] Unabhängige Kabelnetzbetreiber können z.B. Pay-TV-Programme und Pay-per-view-Dienste von der deutschen Pay-TV-Plattform „kabelVision“ beziehen und ausstrahlen. Siehe hierzu: o.V, 2005 (2).

[285] o.V., o.J.(12)

einem Kunden, der das günstigste bzw. das teuerste deutsche Angebot wählt, die in der obigen Tabelle 2 aufgeführten Kosten.

In den Folgejahren fallen lediglich die monatliche digitale Grundgebühr und der Preis für das ausgewählte Pay-Programm an, in den hier aufgeführten Beispielen ist dies eine Summe von 36,-€ bzw. 174,-€ pro Jahr.

Tabelle 3:
Kosten für Kabel Deutschland Pay-TV

Kosten für das billigste Pay-TV-Angebot bei Kabel Deutschland	
Receiver	99,00 €
Freischaltungsgebühr	39,50 €
Smartcard	14,50 €
Programm-Paket "Basic" (12 x 6,-€)	72,00 €
Summe	225,00 €

Kosten für das teuerste deutsche Pay-TV-Angebot bei Kabel Deutschland	
Receiver	99,00 €
Freischaltungsgebühr	39,50 €
Smartcard	14,50 €
Programm-Paket "Basic+Home" (12 x 12,-€)	144,00 €
Summe	297,00 €

Das kostenpflichtige Fernsehangebot bei Kabel Deutschland kostet zwischen 6,-€ im Monat für „Kabel Digital Basic“, welches Premiere „Start“ beinhaltet, und 12,-€ im Monat für die Kombination der Pakete „Basic“ und „Home“.[290] Ausländische Programmpakete kosten zwischen 2,-€ und 22,-€.[291] Ein geeigneter Receiver kostet bei Kabel Deutschland 99,-€, die Smartcard 14,50€. Der Versand des Receivers und der Smartcard erfolgt für den Kunden kostenfrei. Hinzu kommt die Freischaltungsgebühr in Höhe von 39,50€.[292]

Nach der Anschaffung von Receiver und Smartcard ergeben sich in den folgenden Jahren in diesen Beispielen Gebühren in Höhe von 72,-€ bzw. 144,-€ pro Jahr.

Um das Pay-Angebot von Primacom „PrimaTV“ nutzen zu können, muss ein Decoder von Primacom gegen eine Gebühr von 5,95€ im Monat gemietet wer-

---

[286] o.V., o.J.(13)

[287] o.V., o.J.(23)

[288] o.V., o.J.(3)

[289] o.V., o.J.(9)

[290] o.V., o.J.(15)

[291] o.V., o.J.(14)

[292] Auskunft der Kabel Deutschland-Hotline am 01.12.2004, Tel.-Nr.: (0180) 52 333 25

den.[293] Dieser muss in einem Primacom-Shop gegen Hinterlegung einer unverzinsten Kaution von 50,-€ selbst abgeholt werden.[294] Das günstigste Programm-Paket kostet 2,70€ , das teuerste 14,95€ im Monat, einzelne Filme können für 3,95€ abgerufen werden. Bei Nutzung des günstigsten und des teuersten deutschen PrimaTV-Angebots entstehen also jährlich folgende Kosten (Kosten für die Selbstabholung des Receivers werden nicht berücksichtigt, tatsächlich entstehen hierfür u.a. Opportunitätskosten, die vom Zeitaufwand der Abholung abhängen; ebenso vernachlässigt werden die entgangenen Zinsgewinne durch die Kautionshinterlegung):

Tabelle 4:
Kosten für PrimaTV

Jährliche Kosten für das billigste deutsche Pay-TV-Angebot bei Primacom	
Receiver (12 x 5,95€)	71,40 €
Programm-Paket PrimaTV "MTV-Paket" (12 x 2,70€)	32,40 €
Summe	103,80 €

Jährliche Kosten für das teuerste deutsche Pay-TV-Angebot bei Primacom	
Receiver (12 x 5,95€)	71,40 €
Programm-Paket PrimaTV "Maxi plus" (12 x 14,95€)	179,40 €
Summe	250,80 €

Wie bereits erwähnt, kommen bei jeder Bestellung eines Pay-TV-Angebots zusätzliche Kosten wie z.B. Telefongebühren hinzu. Lediglich Primacom bietet hierfür eine kostenfreie Telefonnummer.[295] Der notwendige Zeitaufwand für Bestellung, Besorgung und Installation ist stets individuell anhand der Opportunitätskosten zu bewerten.

4.2. Kosten für den illegalen Zugang zu Pay-TV

4.2.1. Kosten für die Schwarzseher

Um als Schwarzseher rational zu handeln, müssen die Kosten, die dem Schwarzseher für den illegalen Zugang zum Pay-TV-Angebot entstehen, niedriger sein als die Kosten, die für einen äquivalenten regulären Zugang anfallen. Kosten entstehen in Form einmaliger Anfangsinvestitionen und regelmäßig anfallender Kosten. Reguläre Kunden tätigen Anfangsinvestitionen für die erforderliche Hardware des legalen Zugangs wie Decoderboxen, CA-Module, Smartcards, Versandkosten und Aktivierungsgebühren. Laufende Kosten entstehen für die Gebühren und ggf. für die Miete eines Decoders. Schwarzseher benötigen zu Anfang je nach Zugangsmethode Hardware in Form von Decoderboxen, CA-Modulen, Programmiergeräten und Smartcards. Laufende Kosten entstehen

[293] o.V., o.J.(6)

[294] Auskunft der Primacom-Hotline am 02.12.2004, Tel.-Nr.: 0800 - 100 35 05

[295] o.V., o.J.(6)

ihnen hauptsächlich durch die Kosten für notwendige Updates, die in unregelmäßigen Zeitabständen anfallen. Auch zu berücksichtigen sind die Finanzierungskosten, die für die Investitionen in den jeweiligen Zugang entstehen. Wird die benötigte Ausstattung kredit-finanziert, sind entsprechende Zinszahlungen an den Kreditgeber zu leisten. Erfolgt die Bezahlung der Anschaffungen aus vorhandenem Guthaben, sind die Opportunitätskosten zu berücksichtigen: Für den aufgewendeten Betrag ist ein Zinssatz zu ermitteln, der bei alternativer Verwendungsform, beispielsweise bei einer Spareinlage, hätte erreicht werden können.

In Form von Kostengleichungen lässt sich der Zusammenhang folgendermaßen darstellen:

$K_{LZ} = K_{HLZ} + K_G/t * T + FK_{LZ}$

$K_{IZ} = K_{HIZ} + K_U/d * D + FK_{IZ}$

mit

K_{LZ}: Gesamtkosten für legalen Zugang während der Nutzungsdauer T

K_{IZ}: Gesamtkosten für illegalen Zugang während der Nutzungsdauer T

K_{HLZ}: Kosten für erforderliche Hardware des legalen Zugangs inkl. Versandkosten und aller anderen einmaligen Kosten wie Aktivierungsgebühren u.ä.

K_G/t: Kosten für Pay-TV-Gebühren pro Zeiteinheit t (z.B. pro Monat) inkl. aller zusätzlichen regelmäßigen Kosten wie z.B. für die Miete einer Decoderbox

K_{HIZ}: Kosten für erforderliche Hardware des illegalen Zugangs inkl. Versandkosten und aller anderen einmaligen Kosten

K_U/d: Kosten für Updates des illegalen Zugangs pro Durchführung inkl. aller anderen zusätzlichen wiederholt anfallenden Kosten (z.B. digitale Grundgebühr bei Ish)

t: Zeiteinheit

T: Gesamte Nutzungsdauer als $\sum t$

d: einzelne Update-Durchführung

D: Summe aller Update-Durchführungen als $\sum d$

FK_{LZ}: Finanzierungskosten für den legalen Zugang

FK_{IZ}: Finanzierungskosten für den illegalen Zugang.

Es wird davon ausgegangen, dass die zum Empfang benötigte Hardware, wie z.B. eine Decoder-Box oder ein CI-Modul, für die gesamte Zeit der Nutzung des Pay-TV-Angebots funktioniert und daher nur eine einmalige Anschaffung notwendig ist. Sofern für Schwarzseher Kosten für neue illegale Smartcards oder ähnliches anfallen, werden diese unter die Update-Kosten K_U gefasst.

Aus den Gleichungen lässt sich ableiten, dass das Schwarzsehen um so unattraktiver wird, je niedriger die Anschaffungskosten K_{HLZ} und die laufenden Kosten K_G für den legalen Zugang bzw. je höher K_{HIZ} und K_U für den illegalen Zugang sind. Umgekehrt nimmt bei steigenden Beträgen für K_{HLZ} und K_G bzw. sinkenden Beträgen für K_{HIZ} und K_U die Attraktivität des Schwarzsehens zu.

Es gilt:

Wenn $K_{LZ} < K_{IZ}$,

dann ist die Nutzung des legalen Zugangs rational,

wenn $K_{LZ} > K_{IZ}$,

dann ist die Nutzung des illegalen Zugangs rational, und

wenn $K_{LZ} = K_{IZ}$,

dann liegt Indifferenz in der Wahl des Zugangs vor,

unter der Voraussetzung, dass allein das Kostenminimierungsziel ausschlaggebend ist.

Welches Programmangebot ein Schwarzseher nutzen kann, hängt von dem Entschlüsselungscode ab, über den er verfügt.[296] Anhand der oben beispielhaft aufgeführten Pay-TV-Angebote in Deutschland bedeutet dies für einen Schwarzseher, dass die Kosten unter Berücksichtigung der notwendigen Hardware für den illegalen Premiere-Zugang bei einjähriger Nutzung weniger als 216,-€ bei Empfang des Basis-Paketes und weniger als 546,-€ bei Empfang von „Premiere Komplett“ betragen müssen.[297] Entsprechend sollten die Kosten für den illegalen Zugang zum Ish-Pay-TV nicht 134,85€ für die preiswerteste Variante bzw. 272,85€ für Ish-Premium übersteigen, für das Kabel Deutschland-Angebot sollte weniger als 225,-€ („Basic“) bzw. 297,-€ („Basic“+“Home“) und für PrimaTV weniger als 103,80 („MTV-Paket“) bzw. 250,80€ („Maxi-Plus“) aufgewendet werden. Ist der kostenmäßige Aufwand für das Schwarzsehen genauso hoch wie der legale Zugang, liegt bei rein monetärer Betrachtung eine Indifferenz vor, d.h. es macht keinen Unterschied, ob ein legaler oder illegaler Zugang genutzt wird. Entstehen durch das Schwarzsehen jedoch höhere Kosten, ist es rational, auf das reguläre Angebot zurückzugreifen.

Sobald die Hardware einmal angeschafft ist, entstehen für das reguläre Abonnement in der Folgezeit Kosten in Form regelmäßiger Pay-TV-Gebühren und ggf. Receivermiete. Erforderliche Softwareupdates der Smartcards und Decoder erfolgen in der Regel kostenlos und automatisch. Schwarzsehern entstehen Kosten und Opportunitätskosten in Form von Zeit für den Ersatz nicht mehr funktionsfähiger Smartcards oder für Updates des Piraterie-Equipments bei Händlern bzw. durch eigene Downloads aus dem Internet. Entscheidungsrelevant sind dabei immer die Gesamtkosten über eine bestimmte Laufzeit, bestehend aus der Anfangsinvestition und den folgenden laufenden Kosten. Bei-

---

[296] Z.B. gab es bei Premiere bis März 2002 einen einzigen Schlüssel für eine Monitoring-Funktion, mit der für Service- und Demonstrationszwecke auf alle Programme inkl. dem Pay-per-view-Angebot zurückgegriffen werden konnte. Die meisten der illegalen Smartcards verwendeten genau diesen „Händler-Key“. Die Funktion wurde daher abgeschafft. Siehe hierzu o.V., 2002(1) und o.V., 2002(2).

[297] Die Finanzierungskosten des Zugangs werden hier vernachlässigt, da sie nicht pauschal beziffert werden können. Für eine exakte Berechnung im Einzelfall müssen sie zu jeder Zugangsalternative hinzu gerechnet werden.

spielsweise kann eine Schwarzseherlösung trotz höherer Anfangsinvestitionen aufgrund der Einsparung der Abonnement-Gebühren im Zeitablauf billiger sein als das legale Abonnement.

Es gilt:

Wenn $K_{HLZ} > K_{HIZ}$ und $K_G > K_U$, dann gilt immer: $K_{LZ} > K_{IZ}$.

Wenn $K_{HLZ} < K_{HIZ}$ und $K_G < K_U$, dann gilt immer: $K_{LZ} < K_{IZ}$.

Sind also die Kostenbestandteile der einen Nutzungsvariante der anderen stets überlegen, lässt sich eine eindeutige Aussage treffen, welches die billigere und damit rationale Alternative ist. Ist jedoch nur ein Kostenbestandteil überlegen, der andere hingegen unterlegen, sind die entstehenden Gesamtkosten über eine bestimmte Zeitperiode entscheidend.

In der Kostenberechnung sind stets auch die Opportunitätskosten zu berücksichtigen. Diese fallen in Form von Zeitaufwand für die Beschaffung und Installation der technischen Geräte und die Bestellung eines Pay-TV-Abonnements sowie für den Zeitaufwand der erforderlichen Updates an. Die Opportunitätskosten sind auch hier individuell verschieden, da sie auf dem entgangenen Einkommen einer alternativen Beschäftigung beruhen. Im folgenden wird davon ausgegangen, dass die Opportunitätskosten für die Erstinstallation sowohl für den regulären als auch den illegalen Zugang in etwa vergleichbar sind und daher außer Acht gelassen werden können. Opportunitätskosten für spätere Updates der Schwarzsehervariante sind jedoch relevant, da regulären Abonnenten für Updates keine Kosten entstehen, während Schwarzseher hierfür Geld und Zeit aufwenden müssen. Die Opportunitätskosten werden daher in den Update-Kosten berücksichtigt. Grundsätzlich lässt sich jedoch feststellen, dass mit steigenden Opportunitätskosten das Schwarzsehen zunehmend unattraktiver wird: Höhere Opportunitätskosten führen zu steigenden Update-Kosten K_U. Dadurch steigen auch die Gesamtkosten des illegalen Zugangs (K_{IZ}), welche einem fixen Gesamtkostenbetrag des vergleichbaren legalen Zugangs (K_L) gegenüberstehen. Daraus lässt sich ableiten, dass ab einer gewissen Einkommensgrenze des Pay-TV-Nutzers das Schwarzsehen irrational wird.[298]

Beispiel (von den Kosten für die Hardware wird hier wegen der Anschaulichkeit abgesehen): Fallen monatliche Grundgebühren von 5,-€ für ein reguläres Pay-TV-Angebot und im Falle des Schwarzsehens anstatt der Gebühren pro Monat eine Stunde Zeitaufwand für Updates oder ähnliches an, so ist bei einem Stundenlohn von über 5,-€ das reguläre Abonnement die günstigere Alternative, da anstatt des Updates des illegalen Zugangs, welches eine Ersparnis von 5,-€ bewirkt, ein Einkommen von über 5,-€ erzielt werden kann. Betragen die regulären monatlichen Gebühren jedoch 45,-€, muss der Stundenlohn einer alternativen Beschäftigung bereits mehr als 45,-€ betragen, um aus rationalen Gründen auf das reguläre Abonnement zurückzugreifen. Liegt der Stundenlohn unter 45,-€, stellt der illegale Zugang die günstigere Lösung dar, da sich ein höherer

[298] Tatsächlich besteht der Kundenstamm von Premiere überwiegend aus Abonnenten mit überdurchschnittlichem Einkommen. Siehe hierzu: o.V., 2004(2).

Betrag einsparen lässt als durch die alternative Beschäftigung hätte erwirtschaftet werden können.

Welche Kosten für die illegale Nutzung von Pay-TV entstehen, hängt von der Methode des Zugangs ab. Die verschiedenen Varianten des Hackens von Pay-TV werden im folgenden Kapitel dargestellt.

4.2.2. Die Methoden der Pay-TV-Hacker und damit verbundene Kosten für Schwarzseher

Die gegenwärtigen Methoden der Pay-TV-Piraterie setzen überwiegend bei der Decoder-Software und den Smartcards an. Smartcard-Technologie ist in vielen Bereichen der Wirtschaft verbreitet, daher ist die Beschaffung von Hard- und Softwaretools zur Smartcard-Programmierung problemlos möglich.[299] Unter den Pay-TV-Hackern gibt es eine eigene Szene, die sogenannte MOSC-Szene (Modified Original Smartcard), die sich mit dem Hacken von Original-Smartcards, die entweder deaktiviert sind oder nur den Zugang zu einem Basisangebot ermöglichen[300], beschäftigt. Sie manipulieren die Original-Software, welche als Firmware bezeichnet wird. Entweder wird die Firmware verändert oder es werden die als Keys bezeichneten Verschlüsselungscodes, die zwischen der Decoderbox und der Smartcard ausgetauscht werden, abgehört, um sie zusammen mit den übrigen relevanten Daten anschließend auf Blanko-Smartcards zu kopieren.[301] Original-Smartcards können von Hackern mit Hilfe von speziellen Geräten durch Spannungserzeugung „gekillt“ werden, d.h. die ursprünglichen Informationen werden gelöscht. Anschließend können sie mit anderen Daten beschrieben werden. Sobald ein Programmanbieter eine neue Kartenversion mit einer verbesserten Verschlüsselung oder anderen Firmware-Neuerungen herausgibt, kann auf diese Weise eine alte Smartcard „gedumpt“, also auf den neuesten Stand gebracht werden.[302] Derartige Piraten-Smartcards werden auf professionelle Weise mit ökonomisch ausgerichteten Arbeitsmethoden, die Strukturen der organisierten Kriminalität aufweisen, in großer Stückzahl hergestellt und vertrieben. Vereinzelt werden die Karten jedoch auch von technisch versierten „Hobbypiraten“ erstellt und im Bekanntenkreis gegen Geld oder andere Tauschobjekte wie Raubkopien von Software angeboten.[303]

Für einen Schwarzseher bedeutet dies, dass er sich nach Anschaffung eines geeigneten Decoders bzw. CA-Moduls eine illegale Smartcard besorgen muss. Die Karten können z.B. einfach über das Internet bestellt werden. Dafür kann er dann die monatlichen Abonnement-Gebühren einsparen. Sofern für diese Methode reguläre Decoderboxen oder Module verwendet werden können, fallen hierfür die gleichen Kosten an wie bei der Nutzung eines legalen Zugangs und

---

[299] o.V., 2003(3), S. 18

[300] ebenda, S. 18

[301] Nachgebaute Smartcards werden auch als digitale Piraten-Smartcards (DPSCs) bezeichnet. Siehe hierzu: o.V., 2003(3), S. 18.

[302] Hankmann, Sprotte, 2004c, S. 86f.

[303] o.V., 2003(3), S. 18f.

sind daher nicht relevant. Aus monetärer Sicht rational handelt ein Schwarzseher dann, wenn die gehackte Smartcard und der erforderliche Aufwand der Beschaffung geringere Kosten verursachen als ein reguläres Abonnement. In diese Überlegungen müssen eventuelle Updates der Piratenkarte, die durch Codeänderungen der Verschlüsselung seitens des Pay-TV-Senders notwendig werden können, mit einbezogen werden. Entsprechende Keys werden zwar auch kostenlos im Internet veröffentlicht, jedoch muss zum vorher notwendigen Löschen der Karte der Chipspeicher mit speziellen Geräten unter Spannung gesetzt werden, welches spezielles Hacker-know-how voraussetzt und daher als übliche Schwarzseher-Lösung hier nicht in Betracht gezogen wird.[304] Könnte der Schwarzseher z.B. mit Hilfe der illegalen Smartcard auf das „Premiere-Komplett"-Paket zurückgreifen, würde er pro Monat 45,-€ bzw. 540,-€ im Jahr an Abonnementgebühren einsparen. Bei Bestellung des „Premiere-Komplett"-Abos ist eine Decoderbox für 6,-€ erhältlich[305]. Die Gesamtkosten für die Smartcard, deren Beschaffung, die Durchführung der notwendigen Updates und, falls erforderlich, die Beschaffung der notwendigen Hardware, sollten im Jahr demnach weniger als 540,-€ ohne bzw. 546,-€ mit Hardware betragen, liegen sie höher, ist es günstiger, ein reguläres Abonnement abzuschließen. Im Jahr 2001 kostete eine Smartcard für den illegalen Empfang von „Premiere World" auf dem Schwarzmarkt ca. 200,- DM[306] (entspricht 102,26 €). Decoder mit Karte wurden mit bis zu 1000,- DM (entspricht 511,29 €) gehandelt. Dafür muss der Erwerber einer illegalen Karte jedoch in Kauf nehmen, dass beim nächsten Codewechsel das Premiere-Signal im Gegensatz zu den regulären Kunden nicht mehr entschlüsselt werden kann und der Bildschirm daher wieder schwarz bleibt. Bis der Schwarzseher wieder über eine funktionsfähige Karte verfügt, muss er einen Nutzungsausfall in Kauf nehmen, der ihm bei einem regulären Abonnement nicht entsteht. Für eine neue Karte oder ein Update fallen erneut Kosten an.

Die Anwendung illegaler Smartcards wurde in letzter Zeit vermehrt durch die Manipulation von handelsüblichen Decoderboxen oder CI-Modulen abgelöst.[307] Dabei wird die Firmware des Receivers geändert, in der Hacker-Szene wird dies „aufbohren" genannt. Die Hacker entwickeln eine eigene Software, die mit Hilfe von Emulationen das verschlüsselte Signal decodiert. Auch bei diesen Emulationen müssen die Keys regelmäßig erneuert werden. Mit einer ähnlichen Methode konnte der illegale Empfang von Premiere ermöglicht werden, ohne dass dafür eine Smartcard benötigt wurde. Es musste lediglich die Software des CI-Moduls „FreeCam" manipuliert werden.[308] Experten sehen in dieser Hack-

---

[304] Hankmann, Sprotte, 2004c, S. 86f.

[305] Hardwarekosten für das reguläre „Premiere-Komplett"-Abonnement betragen einmalig 6,-€ (1,-€ für den Receiver und 5,-€ Versandkosten).

[306] Der Wert von 8000 beschlagnahmten Smartcards wurde mit einem Verkaufswert von rund 1,6 Millionen Mark angegeben. Dies entspricht einem Preis von 200,- DM pro Karte. Siehe hierzu: Pötzsch, 2001a.

[307] o.V., 2004(5)

[308] Goedecke, Hofmeir, 2003b, S. 37

Methode eine wesentlich größere Gefahr als durch die Smartcardmanipulation. Während für das Löschen und anschließende Verändern der Original-Smartcards immer noch zusätzliche Geräte notwendig sind, die als Umgehungsvorrichtungen laut Gesetz nicht mehr beworben und als solche angeboten werden dürfen, kann eine Emulationssoftware einfach aus dem Internet, derzeit die wichtigste Distributionsplattform der Hacker für Zugangscodes und Updates illegaler Zugangssoftware[309], heruntergeladen und auf den Receiver kopiert werden.[310]

Diese Methode setzt voraus, dass der Hacker sich zunächst eine Decoderbox besorgt, deren Firmware manipulierbar ist. Dies kann die gleiche Decoderbox sein, die er auch für den legalen Zugang nutzen würde, andernfalls muss die Kostendifferenz der unterschiedlichen Decoder berücksichtigt werden. Eine beliebte Box bei Hackern ist die „d-box“ als Linux-Version „Neutrino“.[311] Mittels der Firmwaremanipulation wird das Programm entschlüsselt, so dass auf diese Weise ebenfalls die Abonnementgebühr eingespart werden kann. Der Bezug der erforderlichen Software ist daher in Relation zu den regulären Abonnementgebühren des empfangbaren Programms zu setzen. Im Beispiel des „Premiere-Komplett“-Angebots sollten die Kosten für die Software 45,-€ im Monat bzw. 540,-€ im Jahr nicht überschreiten. Tatsächlich stehen die Software und Angaben zu den aktuellen Keys auch kostenlos im Netz.[312] Daher entstehen nach Anschaffung des Decoders nur noch Opportunitätskosten für die Zeit, die für den Download und die Installation der Software aufgewendet werden muss.[313] Wie bereits erwähnt, sind die Opportunitätskosten individuell in Form des Einkommens einer alternativen Beschäftigung zu ermitteln. Diese sind der ersparten regulären Pay-TV-Gebühr gegenüberzustellen. Wird z.B. ein Zeitaufwand von monatlich 20 Minuten für Updates angenommen, die den Empfang von „Premiere-Komplett“ ermöglichen, entgehen dem Schwarzseher monatlich ein Drittel eines alternativen Stundenlohns. Dies ist der Ersparnis von 45,-€ gegenüberzustellen. Sofern der Schwarzseher über einen Stundenlohn verfügt, der weniger als 135,-€ beträgt, ist die illegale Alternative für ihn rational. Nur wenn er mehr als 135,-€ pro Stunde verdient, ist es günstiger für ihn, gegen 45,-€ im Monat auf Updates zu verzichten und statt dessen einen höheren Betrag zu erwirtschaften. Ermöglicht der illegale Zugang jedoch nur den Empfang von „Premiere Start“ im Wert von 5,-€ im Monat, liegt die Grenze der Opportunitätskosten bei gerade einmal 15,-€ pro Stunde. Könnte der Schwarzseher statt eines Updates innerhalb der 20 Minuten mehr als 5,-€ erwirtschaften, ist es für ihn rational, die regulären Gebühren zu entrichten. Grundsätzlich wird davon ausgegangen, dass der für die Updates notwendige Personalcomputer mit In-

---

[309] o.V., 2003(5)

[310] Hankmann, Sprotte, 2004c, S. 88

[311] Hankmann, Sprotte, 2004b

[312] z.B. auf http://www.la-cafetera.com (Stand: 08.12.2004)

[313] Kosten für die Nutzung der Telefonleitung während des Downloads betragen nur wenige Cents und werden daher außer Acht gelassen.

ternetanschluss im Haushalt des Hackers bzw. Schwarzsehers bereits vorhanden ist, so dass diese Anschaffung bei den Kosten nicht berücksichtigt wird.[314]

Einige Piraten setzen bei der Suche nach Methoden für den freien Pay-TV-Empfang noch früher an, nämlich direkt beim Verschlüsselungssystem. Sie basteln sich eigene Module, die einzelne oder auch mehrere Verschlüsselungssysteme gleichzeitig emulieren können. Solche Module sind unter den Namen „JokerCam“, „UniversalCam“ oder „KidCam“ bekannt.[315] Das bekannteste dieser Art ist das „Magic Modul“. Diese CAMs werden ohne Software und damit ohne Funktionen ausgeliefert und als „Programmierplattform für eigene Softwarelösungen“ deklariert.[316] Pay-TV-Piraten laden nach dem Erwerb die benötigte Software zum Entschlüsseln der Programme aus dem Internet und programmieren damit die Module.[317] Dazu wird der PC mit dem sogenannten „Programmer“ verbunden, der zur Programmierung wie eine Smartcard in das Modul gesteckt wird.[318] Da durch das Gehäuse der Module Patent- und Lizenzbestimmungen verletzt werden, ist das Bewerben und der Verkauf dieser Produkte nicht mehr erlaubt. Auch durch die Programmierung der Module mit der illegalen Entschlüsselungssoftware werden Urheberrechte verletzt und damit eine Straftat begangen.[319]

Bei dieser Methode wird die Hardware, nämlich das CA-Modul ausgetauscht. Es ist also zunächst festzustellen, welche Preisdifferenz zwischen dem regulären CA-Modul bzw. einer entsprechenden Decoderbox auf der einen Seite und einem Decoder mit CI-Schacht zzgl. des Piraten-CA-Moduls und eines notwendigen Programmiergerätes, dem sogenannten „Programmer“, auf der anderen Seite vorliegt. Eventuell ist für den Empfang der Sender dann noch eine Smartcard notwendig. Hierzu werden Blanko-Smartcards wie z.B. „Goldwafer“ oder „Silverwafer“ benutzt.[320] Im Anschluss daran ist wiederum die eingesparte Abonnementgebühr der dann empfangbaren Programme zu kalkulieren. Rational ist das Schwarzsehen dann, wenn die Summe der Hardware des Piraterie-Equipments geringer ist als die Summe der legalen Hardware zzgl. der Pay-TV-Gebühr. Dabei ist zu berücksichtigen, inwiefern die CA-Module Updates benötigen und mit welchen Kosten dies verbunden ist. Illustriert am Beispiel von „Premiere-Komplett“ bedeutet das: im Jahr der Anschaffung sollten für Decoderbox,

---

[314] Lt. Stat. Bundesamt verfügten im Jahr 2003 61% der privaten Haushalte in Deutschland über einen PC, 42,6% nutzten das Internet oder Online-Dienste, jeweils mit steigender Tendenz. Da einem Schwarzseher oder Hacker eine hohe Technik-Affinität unterstellt werden kann, ist die Wahrscheinlichkeit hoch, daß er zu der Gruppe gehört, die über einen PC mit Internet-Anschluß verfügt. Siehe hierzu: o.V., 2004(9).

[315] Goedecke, Hofmeir, 2003b, S. 37

[316] o. V., 2002(13)

[317] o.V., 2002(12)

[318] o .V., o.J.(16)

[319] o. V., 2002(13)

[320] Hankmann, Sprotte, 2004b

Piraten-CA-Modul und eventuelle Updates weniger als 546,-€ anfallen, in den Folgejahren für Updates weniger als 540,-€. Hinzu kommen die Opportunitätskosten für den Zeitaufwand der Updates, die bei einem regulären Abonnement entfallen. Der Download der Hack-Software und die Programmierung des Moduls dauern auch hier nur einige Minuten.

Ungeachtet des Verbots der Bewerbung und des Verkaufs der frei programmierbaren CAMs zu gewerblichen Zwecken sind sie weiterhin erhältlich. Beim Online-Auktionshaus ebay war beispielsweise ein Magic Modul mit Programmer und Software für einen Sofort-Kauf-Preis von 89,-€ zzgl. 10,-€ Versandkosten erhältlich.[321] Für den Anschluss des Programmers an den Computer ist ein serielles Verbindungskabel notwendig,[322] welches für 3,49€ zu erwerben ist.[323] Die Programmier-Software, sogenannte „Loader Programme“ wie „Pentasoft“ oder „Pentacrypt“, gibt es kostenlos im Internet.[324] Auf den Internetseiten wird auch Schritt für Schritt erklärt, wie die Software und Hardware zu verwenden sind.[325] Die entstehenden Verbindungskosten für den Software-Download sind vernachlässigbar gering. Blanko-Smartcards kosten wenige Euro, z.B. ist eine Goldwafer-Karte für 3,-€ zu bekommen.[326] Den Anschaffungskosten eines regulären Abonnements stehen für die Schwarzseher-Lösung also 105,49€ gegenüber. Kosten für die Updates resultieren auch hier aus den individuellen Opportunitätskosten des benötigten Zeitaufwands.

Eine weitere Variante, um Verschlüsselungen zu überlisten, ermöglicht es derzeit, Premiere gebührenfrei zu empfangen, obwohl das verwendete Verschlüsselungssystem noch nicht geknackt wurde. Dabei werden die Daten einer Original-Premierekarte über einen Cardsharing-Server an die Nutzer verteilt, so dass das Programm über Internet empfangen werden kann. Allerdings ist diese Methode zum einen mit erheblichem technischen Aufwand verbunden, zum anderen kann mittels der IP-Adresse jeder Schwarzseher identifiziert werden. Da-

---

[321] Private ebay-Versteigerung vom 27.11.2004, URL: http://cgi.ebay.de/ws /eBayI SAPI.dll?ViewItem&category=15067&item=5734752092&rd=1. Es existieren auch ähnliche gewerbliche Angebote.

[322] o.V., o.J.(16)

[323] Angebot bei „Sat Place“ unter http://satplace.de/spnew/frontend /index.php?disp= pdetail&id=106&cat=14&parent=&s=newsess&prxcnt=1&err=url_secure_not_found-&PHPSESSID=3b0fbb013f5f1f6a1f36b6896c90ad1b (Stand: 20.02.2005).

[324] z.B. bei: http://www.digisatshop.ch/de-ch/dept_17.html (Stand: 08.12.2004) oder: http://www.la-cafetera.com/magic-soft.htm (Stand: 08.12.2004) oder auch: http:// www.cam-modul.info/magiccam/seiten/seite_31.htm (Stand: 09.12.2004).

[325] z.B. ist auf der Internet-Seite http://www.cam-modul.info/magiccam/seiten /seite_2.htm eine genaue Anleitung der Programmierung des Magic Moduls zu finden (Stand: 09.12.2004).

[326] Angebot des „Wafer-Shop Duisburg“ vom 23.12.2004 im Internet unter der URL: http://www.wafer-shop.de/shop./?action=list&command=selectCategory&component=categoryTree&categoryId=3f55db8bdba46&sid=9b50cc3e4afc6ae4661-bfeacbcf43234&sid=9b50cc3e4afc6ae4661bfeacbcf43234

her gilt diese Methode unter den Piraten als nicht mehr aktuell und wird in den einschlägigen Internetforen auch nicht mehr diskutiert.[327]

Vor der Verschlüsselungsumstellung, als Premiere das Codiersystem Irdeto/ Betacrypt verwendete, wurde das Programm sehr häufig am Computer per Softdecodierung entschlüsselt. Dazu wurden lediglich eine DVB-PC-Karte und eine Software, die im Internet zur Verfügung stand, benötigt. Zusätzliche Hardware wie CA-Module oder Smartcards waren nicht erforderlich.[328] Statt dessen wurde von Hackern ein Software-Tool entwickelt, welches den Verschlüsselungsalgorithmus durch Emulation umging. Die hierfür benötigten PC-TV-Karten kosteten etwa 220,-€. Die zusätzlich notwendige Software konnte kostenlos bezogen werden. Sie musste im Anschluss nur um eine spezielle DLL-Datei erweitert werden, welche ihr die Fähigkeit verlieh, ein CI-Modul zu emulieren. Nach wenigen Einstellungen konnte per PC Pay-TV empfangen werden. Nicht nur Premiere, sondern auch alle anderen Sender, die über Irdeto/Betacrypt oder Seca/Mediaguard verschlüsselten, konnten auf diese Weise decodiert werden.[329] Sogar die Pay-per-view-Angebote ließen sich durch die Software freischalten. Mit Hilfe des sogenannten „IPPV Tools“ konnte auf einer originalen Smartcard das Pay-per-view Guthaben, mit welchem die Filme bezahlt wurden, immer wieder kostenlos aufgeladen werden.[330]

Für eine vergleichbare legale Variante, um Premiere am PC zu empfangen, wurde neben einer PC-Karte mit Common Interface für ca. 200,-€ ein Common-Interface-Zusatz für etwa 100,-€ und ein Irdeto/Betacrypt-CA-Modul für rund 200,-€ benötigt. Nach dieser 500,-€-Anfangsinvestition musste noch ein reguläres Abonnement abgeschlossen werden, welches mit monatlichen Kosten verbunden war. Die illegale Variante benötigte dagegen nur die PC-TV-Karte für etwa 200,-€ und ermöglichte kostenfreien Empfang mehrerer Pay-Sender.[331] Die Schwarzseher-Variante wies hier also einen deutlichen Kostenvorteil auf. Für die aktuelle Verschlüsselung von Premiere ist eine solche illegale Empfangsmöglichkeit jedoch gegenwärtig nicht bekannt.

Eine andere Methode für Schwarzseher ist der Bezug der Filme über das Internet. Empfänger von Pay-TV speichern das ausgestrahlte Filmmaterial in digitaler Form auf Festplatte, entweder auf dem eigenen Computer oder auf einem digitalen Festplattenrecorder, und bieten den Film anschließend im Internet, z.B. in einer Tauschbörse an. Handelt es sich um Kinofilme, die bereits gelaufen sind und eventuell schon auf DVD oder Video veröffentlicht wurden, sind nur geringe Auswirkungen zu erwarten, da der Film wahrscheinlich schon seit längerer Zeit im Internet verfügbar ist. Handelt es sich jedoch um Programminhalte, die durch den Sender zum ersten Mal exklusiv ausgestrahlt werden, so

---

[327] Hankmann, Sprotte, 2004c, S. 88

[328] o.V., 2002(3)

[329] Scheffel, 2002

[330] o.V., 2002(3)

[331] Nickles, 2002

stellt diese Form des Schwarzsehens eine relevante Bedrohung dar. Die zunehmende Verbreitung von Breitband-Internetanschlüssen in Kombination mit einer Zugangsflatrate in den privaten Haushalten macht das Downloaden auch größerer Dateien wie die von Filmen zu keinem Problem mehr. Da bei dieser Form des Schwarzsehens neben dem Breitband-Internetanschluß und dem Computer kein zusätzlich notwendiges Equipment notwendig ist, fallen für den Schwarzseher nur Opportunitätskosten für den Zeitaufwand an, den er zum Suchen des gewünschten Filmes im Internet aufwenden muss. Über Suchmaschinen und Tauschbörsen genügen meist wenige Clicks bis zum Download. Mögliche Probleme sind hierbei, dass ein gewünschter Film nicht in Internettauschbörsen angeboten wird oder ein Downloadvorgang nicht oder nur schlecht funktioniert. Auch Bild- und Tonqualität sind nicht immer gut. Zudem beinhalten Downloads immer auch das Risiko des Einfangens von Viren, Trojanern o.ä. Darüber hinaus kann anhand der zugewiesenen IP- und DNS-Adresse der Internetzugang des Nutzers festgestellt und der Schwarzseher entdeckt werden.

Unabhängig von der Methode, die für den illegalen Pay-TV-Empfang angewendet wird, muss in jedem Fall auf Garantieansprüche oder zusätzlichen Service wie Hotlines durch die Pay-TV-Sender verzichtet werden. Das erhaltene Leistungspaket ist also im Schwarzseher-Fall nicht exakt das gleiche wie bei einem regulären Abonnement.[332]

4.2.3. Kosten und Nutzen für Hersteller und Dealer von Piraterie-Equipment

Aus ökonomisch rationalen Überlegungen sollten sowohl für den Hersteller als auch für den Distributor der Herstellungs- bzw. Beschaffungsaufwand kostenmäßig geringer sein als der Vertrieb der Produkte. Software-Hacker investieren vor allem Zeit in das Knacken der Codes. Dazu benötigen sie die entsprechende Computerausstattung, die von Zeit zu Zeit auf den neuesten Stand gebracht werden muss. Computertechnologie unterliegt dabei kurzen Innovationszyklen. Zum einen werden Hard- und Software für Hacker immer leistungsfähiger, zum anderen fallen auch die Preise für das Equipment permanent, so daß der Hacker mit relativ geringem Kostenaufwand stets über leistungsfähige Technologie verfügt.[333] Wird eine Software für Smartcards entwickelt, installiert der Hacker diese auf programmierbaren Karten und vertreibt sie entweder selbst direkt über das Internet oder über Zwischenhändler. Illegale Smartcards können auf dem Schwarzmarkt hohe Preise erzielen und sind daher für die Piraten finanziell attraktiv.[334] Dient die Cracksoftware zur Manipulierung von Decodern, kann sie kostengünstig auf einem Internet-Server bereitgestellt und gegen die Zahlung eines Entgeltes zum Download angeboten werden. Der Verdienst wäre dann von der Anzahl der Abrufe abhängig. Dabei besteht die Gefahr, dass die Software von einem Nutzer auf einem anderen Webserver gegen ein geringeres Entgelt oder sogar kostenlos bereitgestellt werden kann. Urhe-

---

[332] Pötzsch, 2001c

[333] Vgl. o.V., 2003(8).

[334] Vgl. o.V., 2004(5).

berrechtsverletzungen und Androhungen von Rechtsmitteln durch den Hacker scheinen hierbei unwahrscheinlich, schließlich dient die Software selbst keinem legalen Zweck. Wird Decodierungshardware manipuliert, müssen mit dem Verkauf der Smartcards, Decoderboxen und CI-Module sowohl die Beschaffungskosten als auch der Zeitaufwand für die Entwicklung und Implementierung der Software bzw. Firmware abgegolten werden. Zusätzlich muss das eingegangene Risiko durch die illegalen Tätigkeiten angemessen entschädigt werden. Dabei muss der Verkaufspreis den Preis legaler Geräte in Verbindung mit Abonnementkosten unterbieten, da ansonsten ein legaler Zugang für den Nutzer attraktiver ist. Neben dem Verkauf seiner Piraten-Ware kann ein Hacker auch zusätzliche Einnahmen generieren, z.B. indem er kostenpflichtigen Werbeplatz auf seiner Homepage anbietet.

Viele Hacker handeln jedoch nicht aus wirtschaftlichen Gründen. Oft geht es Ihnen nur darum, der Öffentlichkeit ihre technischen Fähigkeiten zu demonstrieren. Ihre entwickelte Software stellen sie dann kostenlos zur Verfügung.[335] Viele von ihnen versprechen sich davon auch, gerade die Aufmerksamkeit der Pay-TV- und Verschlüsselungsanbieter zu gewinnen. Kontakte zu Hackern gehören nämlich laut einer NDS-Sprecherin zur normalen Informationsbeschaffung dieser Firmen.[336] Diese Art der Informationsanfragen können für Hacker lukrative Einnahmequellen darstellen. Oftmals wird den Hackern auch angeboten, die Seite zu wechseln und gegen ein attraktives Gehalt für die eigene Firma am Schutz gegen Piraterie zu arbeiten.

Dealer von Piraten-Technik beziehen ihren Verdienst aus der Gewinnmarge der verkauften illegalen Smartcards und Entschlüsselungsgeräte, der Verkaufspreis liegt also über dem Einkaufspreis. Gewinne erzielen sie auch aus dem Verkauf von Blanko-Smartcards und Programmiergeräten oder sogar von kompletten Satelliten-Empfangsanlagen, zu denen Piratenkarten zu günstigen Konditionen angeboten werden, die zuvor vom Dealer entweder selbst hergestellt oder von professionellen Smartcard-Piraten bezogen wurden.[337] Ebenfalls können zusätzliche Einnahmen durch Werbebanner auf der eigenen Webseite generiert werden. Auf der Kostenseite stehen für Großhändler von Piraterie-Hardware neben den regulären Einkaufs- und Betriebskosten auch Subventionen für Speicherplatz auf Internet-Servern, auf denen illegale Zugangscodes und Anleitungen für diese Hardware bereitgestellt werden.[338] Sämtliche Einnahmen müssen nicht nur dazu dienen, alle anfallenden Kosten zu decken, sondern auch eine Risikoprämie enthalten. Da der Verkauf des Piraterie-Equipments verboten ist und unter Strafe steht, die seine Freiheit kosten kann, geht der Verkäufer ein hohes, sogar existentielles Risiko ein.

---

[335] o.V., 2001b

[336] Röttgers, 2002

[337] o.V., 2003(3), S. 19

[338] o.V., 2003(9), S. 4

Langfristig kann angeführt werden, dass sowohl Hersteller als auch Vertreiber von Piraterie-Soft- und -Hardware sich selbst ihre Geschäftsgrundlage zerstören. Durch das Schwarzsehen werden die Pay-TV-Anbieter um ihre Einnahmen gebracht. Bei einem Einnahmenniveau, das nicht mehr kostendeckend ist, müssen diese den Betrieb einstellen. Dann bleibt auch für die Schwarzseher der Bildschirm schwarz und für Hacker-Equipment gibt es keinen Bedarf und auch keine Nachfrage mehr.[339] Zu beachten ist dabei jedoch, dass die Alternative für den Hacker, sich deshalb aus dem Piraterie-Geschäft zurückzuziehen, das sofortige Ende seines Geschäftes bedeuten würde und daher ökonomisch nicht logisch ist. Als Eigennutzen-Maximierer handelt er allein aus individuell rationalen Gründen, d.h., solange er Gewinne erzielen kann, wird er sie daher auch abschöpfen. Lediglich ein erhöhtes Strafmaß bzw. eine erhöhte Entdeckungswahrscheinlichkeit aufgrund vermehrter Fahndungsaktivitäten oder ähnliches könnte dazu führen, dass einem Hacker die in seinem Gewinn enthaltene Risikoprämie nicht mehr hoch genug erscheint und er sich daher aus dem illegalen Betätigungsfeld zurückzieht.

4.3. Risiken durch Schwarzsehen

Bei der Analyse der Kosten für das Schwarzsehen dürfen nicht nur die Kosten für Hardware und Abonnementgebühren betrachtet werden. Denn bevor ein potentieller Schwarzseher illegal Programme entschlüsseln kann, muss er erhebliche Risiken eingehen, die bei der Kosten-Nutzen-Analyse unbedingt Berücksichtigung finden müssen.

4.3.1. Technische Risiken des Schwarzsehens

Piratensoftware, die aus dem Internet heruntergeladen wird, kann z.B. Viren beinhalten, die unter Umständen den eigenen Computer lahmlegen oder wichtige Daten zerstören können. Auch Dialer können auf diese Weise auf der Festplatte platziert werden und so für teure Telefonrechnungen sorgen. Ebenso kann die illegale Software die CI-Module oder Decoderboxen schädigen. Beispielsweise zerstörte Pentacrypt, eine Software für das sogenannte „Magic Modul“, alle Module, die nicht von einem bestimmten Hersteller stammten. Die Wiederherstellung des Moduls konnte daraufhin nur noch kostenpflichtig durch einen Fachmann erfolgen.[340] Außerdem müssen Nutzer des Magic Moduls damit rechnen, dass das Modul durch Anbieter von Conditional-Access-Systemen via Satellit dauerhaft außer Funktion gesetzt und damit wertlos wird.[341] Risiken sind auch mit dem Bezug von Smartcards oder Modulen verbunden, die angeblich noch nicht geknackte Verschlüsselungen überwinden können. Diese können einige hundert Euro kosten und sind im günstigsten Fall wirkungslos.[342]

---

[339] Vgl. o.V., 2002(9).

[340] Hankmann, Sprotte, 2004f.

[341] o.V., 2002(8)

[342] Hankmann, Sprotte, 2004f.

Grundsätzlich können im Falle defekter Piraterie-Hardware oder bei angerichteten Schäden durch illegale Software keine Garantie- oder Regressforderungen gestellt werden, das Risiko liegt beim Anwender. Auch auf Serviceleistungen durch den Sender wie z.B. Hotlines für technische Probleme muss ein Schwarzseher verzichten.

4.3.2. Rechtliche Konsequenzen für Pay-TV-Piraten

Eines der größten Probleme hinsichtlich der Piraterie ist die öffentliche Wahrnehmung des Themas. Die unberechtigte Nutzung von immateriellen Gütern wird weithin als Kavaliersdelikt angesehen. Im Zusammenhang mit der Verbreitung von Multimedia-fähiger Hardware wird die Piraterie zu einer allgemein akzeptierten Praxis.[343] Dass es sich bei der Piraterie um strafbare Gesetzesverstöße handelt, denen ernsthafte Konsequenzen folgen können, ist vielen nicht bewusst. Pay-TV-Piraterie ist illegal und damit strafbar. Piraten gehen das Risiko ein, bei Entdeckung mit einer erheblichen Strafe belegt zu werden.

Das Vorgehen gegen Schwarznutzer, die sich mit Hilfe von gefälschten Smartcards, manipulierten Originalkarten oder auf eine andere Art Zugang zu kostenpflichtigen Diensten erschleichen, stößt im allgemeinen auf keine größeren rechtlichen Hindernisse.[344] Dabei spielen strafrechtliche, wettbewerbsrechtliche und urheberrechtliche Gesetzesbereiche eine Rolle[345] sowie im gewerblichen Bereich auch das Zugangskontrolldiensteschutz-Gesetz.[346]

Schwarzsehen ist eine Straftat. Nach § 202a Abs. 1 StGB wird derjenige mit einer Freiheitsstrafe bis zu drei Jahren oder mit einer Geldstrafe bestraft, der „unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft“. Die Zugangserschleichung mittels manipulierter oder verfälschter Smartcards ist Computerbetrug nach § 263a StGB, da unbefugt auf den Ablauf einer Datenverarbeitung eingewirkt wird.[347] Hierfür droht eine Geldstrafe oder eine Freiheitsstrafe bis zu fünf Jahren. Auch einer Leistungserschleichung nach § 265a StGB kann sich ein Schwarzseher schuldig machen[348], die mit Geldstrafe oder Freiheitsentzug bis zu einem Jahr bestraft werden kann, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Nicht eindeutig ist dagegen, ob auch ein Vergehen nach den §§ 269 und 270 StGB vorliegt. Damit diese Paragraphen greifen, muss eine Piratenkarte beweiserhebliche Daten enthalten, die ein Rechtsverhältnis bestätigen. Meistens sind auf einer Smartcard jedoch nur Sendeinformationen und Entschlüsselungscodes zu finden, aber keine Zugangsberechtigung im eigentlichen Sinne. Damit ist die Beweiserheblichkeit der gespeicherten Informationen nicht gegeben. Der Pay-TV-Sender kann darüber

---

[343] o.V., 2004(8)

[344] o.V., o.J.(19)

[345] Vgl. Große Peclum, 1991, S. 81.

[346] Hofmeir, 2003b

[347] o.V., o.J.(19)

[348] ebenda

hinaus Schadensersatzansprüche geltend machen gemäß § 823 Abs. 2 (BGB) in Verbindung mit Schutzgesetzen, gemäß § 826 Abs.1 BGB bei vorsätzlicher sittenwidriger Schädigung und in Einzelfällen auch nach § 280 Abs. 1 BGB, sofern ein Vertragsverhältnis besteht.[349]

Neben dem StGB und dem BGB ist auch das Gesetz gegen den unlauteren Wettbewerb (UWG) relevant. Nach § 17 UWG droht demjenigen, der „zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, sich ein Geschäfts- oder Betriebsgeheimnis durch Anwendung technischer Mittel [...] unbefugt verschafft oder sichert oder [...] durch eine eigene oder fremde Handlung [...] erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt," eine Freiheitsstrafe bis zu drei Jahren oder eine Geldstrafe. Die geschützten Keys und Algorithmen der Verschlüsselung sind solche Geschäfts- und Betriebsgeheimnisse.[350] Bereits der Versuch ist strafbar. In besonders schweren Fällen beträgt die Freiheitsstrafe sogar bis zu fünf Jahren. Ein besonders schwerer Fall liegt vor, „wenn der Täter gewerbsmäßig handelt [oder] bei der Mitteilung weiß, dass das Geheimnis im Ausland verwertet werden soll oder eine Verwertung [...] im Ausland selbst vornimmt".

Darüber hinaus liegt beim Schwarzsehen ein Verstoß gegen das Urheberrecht vor. Jegliche Art von Programminhalten ist urheberrechtlich geschützt. Der Urheber verfügt ausschließlich über das Recht der Vervielfältigung, Verbreitung, Bearbeitung, öffentlichen Wiedergabe und Umgestaltung. Sollen diese Tätigkeiten von anderen Personen durchgeführt werden, muss der Urheber dem zustimmen. Die Missachtung des Urheberrechtsgesetzes wird gemäß §§ 106, 108 UrhG mit einer Freiheitsstrafe von bis zu drei Jahren oder einer Geldstrafe bestraft.[351] Werden technische Maßnahmen, die dem Schutz urheberrechtlicher Werke dienen, ohne Zustimmung des Rechtsinhabers umgangen, beispielsweise durch die Nutzung illegaler Smartcards, liegt ein Verstoß gegen § 95a Abs. 1 UrhG vor. Dieser kann zivilrechtliche Unterlassungs-, Schadensersatz- und Vernichtungsansprüche nach sich ziehen.[352] § 95a Abs. 3 verbietet unter anderem die Herstellung von Umgehungseinrichtungen, auch zu privaten Zwecken. Ebenso ist die Einfuhr derartiger Vorrichtungen durch Privatpersonen untersagt. Lediglich der Besitz zu nicht gewerblichen Zwecken fällt nicht unter das Verbot.[353] Der Verkauf, die Vermietung oder die Verbreitung der Umgehungsmittel über den persönlich verbundenen Bekanntenkreis hinaus kann mit einem Bußgeld von bis zu 50.000,- Euro geahndet werden.

---

[349] ebenda

[350] Hankmann, Sprotte, 2004c, S. 88f.

[351] Vgl. ebenda, S. 89.

[352] Bechtold, 2004, S. 26

[353] ebenda, S. 38

Ebenfalls relevant ist das Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (ZKDSG).[354] Die Verschlüsselung ist eine solche Zugangskontrolle, da durch sie nur ein durch Zahlung berechtigter Personenkreis Zugang zu dem verschlüsselten Programm haben soll. Das Gesetz sieht eine Geldstrafe oder Freiheitsentzug von bis zu einem Jahr vor, wenn sogenannte Umgehungsvorrichtungen zu gewerbsmäßigen Zwecken hergestellt, eingeführt oder verbreitet werden. Unter das Verbot fallen auch der Besitz, die technische Einrichtung, die Wartung und der Austausch zu gewerbsmäßigen Zwecken, welche mit einem Bußgeld von bis zu 50.000 Euro geahndet werden können, sowie die Absatzförderung der Umgehungsvorrichtungen. Unter Umgehungsvorrichtungen versteht der Gesetzgeber technische Verfahren oder Vorrichtungen, die die unerlaubte Nutzung eines zugangskontrollierten Dienstes ermöglichen. Dazu gehören Computerprogramme zum Auslesen von Daten oder Geräte, sogenannte Progger, mit denen Blanko-Smartcards beschrieben werden können.[355] Der Gesetzgeber betont, dass gegen das ZKDSG bereits dann verstoßen wird, wenn eine Vorrichtung nur unter anderem der Umgehung dient. Dadurch soll verhindert werden, dass das Gesetz durch Software und Geräte mit gemischten Funktionen umgangen werden könnte.[356] Diese Geräte dürfen nun also nicht mehr beworben oder vertrieben werden.[357] Straffrei ist nach dem ZKDSG allerdings der Erwerb der Umgehungsvorrichtungen, z.B. CAMs wie das Magic Modul oder Software wie Pentacrypt, durch Privatpersonen für den eigenen Besitz, da in diesem Fall kein gewerbsmäßiger Zweck verfolgt wird. Ebenso nicht unter das Gesetz fällt der Verkauf von Umgehungsvorrichtungen durch Privatpersonen zu nicht gewerbsmäßigen Zwecken. Sobald jedoch die Software in dem Modul installiert wird, werden geltende Patente und Lizenzbestimmungen verletzt, da die Verschlüsselungsfirmen nur bestimmte Firmen, zumeist SCM Microsystems, mit der Produktion der Module beauftragt haben.[358] Gegenwärtig versucht die AEPOC, innerhalb der EU ein Verbot auch für den Besitz und den persönlichen Gebrauch von illegalen Decodiergeräten durchzusetzen.[359]

4.3.3. Verfolgung von Pay-TV-Piraten

Bundesweite Polizeiaktionen haben in der Vergangenheit bereits zu zahlreichen Durchsuchungen von Wohnungen und Büros geführt. Im Zuge dieser Maßnahmen konnten u.a. mehrere Tausend illegale Smartcards sichergestellt werden.[360] Im Jahr 2002 wurde ein Dealer zu zwei Jahren Haft verurteilt, der mit gehackten Premiere-Smartcards und unterschlagenen Digitalreceivern gehan-

---

[354] Hofmeir, 2003a, S. 16f.

[355] Hankmann, Sprotte, 2004c, S. 89

[356] Hofmeir, 2003a, S. 16

[357] Hankmann, Sprotte, 2004c, S. 89

[358] o.V., 2002(12)

[359] o.V., 2004(5)

[360] o.V., 2002(6).

delt hatte.[361] Die Ermittlungen richteten sich dabei nicht nur gegen die Vertreiber, sondern auch gegen die Abnehmer des Piraten-Equipments. Beispielsweise konnten die Fahnder Abnehmer von Piraterie-Produkten, die die Ware über Internetauktionshäuser erworben hatten, ausfindig machen. Auch deren Wohnungen wurden daraufhin durchsucht.[362] Schwarzseher und Pay-TV-Hacker werden außerdem oft durch anonyme Anzeigen aus dem Bekanntenkreis oder von unzufriedenen Abnehmern der illegalen Zugänge entdeckt. Solche Hinweise ziehen ebenfalls Hausdurchsuchungen der Beschuldigten nach sich, bei denen Hack-Equipment und Piratenkarten sichergestellt werden.[363]

Werden im Rahmen einer Hausdurchsuchung Hard- und Software für den illegalen Empfang von Pay-TV gefunden, werden diese Gegenstände beschlagnahmt. Der betroffene Pirat erhält dafür natürlich keine Gegenleistung oder Entschädigung, so dass das investierte Geld in diese Geräte und Programme verloren ist. Neben Smartcards, Kartenlesegeräten oder Decodern wird meistens auch der private Computer beschlagnahmt, auf den der Betroffene dann zumindest zeitweise nicht mehr zurückgreifen kann.[364] Sofern er auf Grund seiner Vergehen nicht inhaftiert ist, kann daher die Neuanschaffung eines Computers notwendig werden. Sollte die Entdeckung eines Hackers oder Dealers zu Freiheitsentzug führen, kann er auch andere Beschäftigungen, die er eventuell zusätzlich zu seinen Betätigungen im Pay-TV-Geschäft betrieben hat, nicht mehr ausüben, eventuell ist ein Verlust seines Arbeitsplatzes die Folge. Das bedeutet, er muss nicht nur auf die Einnahmen seines Pay-TV-Geschäfts verzichten, sondern auch auf das Einkommen anderer Tätigkeiten.

Die Verfolgung der Pay-TV-Piraten soll in Zukunft vor allem über die Ländergrenzen hinweg weiter intensiviert werden. Gemäß der „Deklaration des Europäischen Parlaments zur Bekämpfung der Piraterie und Fälschungen in der erweiterten EU“ wird in Zukunft die Zusammenarbeit der Behörden auf grenzüberschreitender Ebene und die Rolle von Europol verstärkt. Gleichzeitig sollen in allen Mitgliedsländern Urheberrechtsverletzungen strikt verfolgt und vor allem in Fällen mit kommerziellem Hintergrund hart bestraft werden.[365]

Auch im Ausland wird die Verfolgung der Pay-TV-Piraten betrieben. In Italien verfügt die Polizei über eine eigene Einheit mit 2000 speziell ausgebildeten Beamten, die neben Computer- und Telekommunikationsvergehen auch für die Pirateriebekämpfung zuständig ist. In der Türkei gelang es dem Pay-TV-Sender Digitürk, Abonnenten ausfindig zu machen, die ihre Smartcard manipuliert hatten. Daraufhin wurden die Abonnenten mit Geldstrafen belegt.[366] In den USA wurden Dealer, die über das Internet Piraten-Equipment angeboten hatten, aus-

---

[361] o.V., 2002(7)

[362] o.V., 2002(6)

[363] Vgl. Hofmeir, 2003b.

[364] Pötzsch, 2001b

[365] McCarthy u.a., 2003

[366] o.V., 2003(5)

findig gemacht und deren Kundenlisten beschlagnahmt. Anschließend wurden diesen Kunden Abmahnungen mit hohen Geldforderungen zugestellt und einige hundert Prozesse gegen sie angestrengt.[367]

4.3.4. Das Entdeckungsrisiko der Pay-TV-Piraten

Auch wenn die Gesetzeslage eindeutig ist, werden Pay-TV-Anbieter nur in den seltensten Fällen Schwarzseher identifizieren und zur Rechenschaft ziehen können.[368] Im Jahr 2001 gab es gerade einmal 300 Verfolgungen aufgrund des Kopierens von Pay-TV-Karten.[369]

Die Wahrscheinlichkeit, Programmierer und Anbieter von Hack-Software, die ihre Programme im Internet kostenlos zum Download bereitstellen, ausfindig zu machen, ist äußerst gering. Oft wird die Software auf Servern im Ausland bereitgestellt, so dass eine länderübergreifende Zusammenarbeit der Sicherheitsbehörden notwendig wäre. Diese ist sehr aufwendig, und nur mit wenigen Ländern ist derzeit eine effektive Kooperation möglich. Daher stehen die von den Hackern verwendeten Server zumeist in Ländern, in denen eine Strafverfolgung unwahrscheinlich ist. Da es durch das kostenlose Bereitstellen der Software zu keinen Zahlungsströmen kommt, ergeben sich auch keine verwertbaren Verfolgungsspuren, die zu dem Hacker führen könnten. Internetnutzer, die sich illegale Hacker-Tools aus dem Internet lediglich herunterladen, machen sich im Gegensatz zu den Anbietern der Software nicht strafbar.[370]

Für eine rationale Bewertung des juristischen Risikos, das er durch das Schwarzsehen eingeht, muss ein Pay-TV-Pirat folgende Überlegung anstellen: Das Risiko, entdeckt zu werden, muss mit der Höhe der drohenden Strafe multipliziert werden. Wie gering die Wahrscheinlichkeit einer Strafverfolgung für Pay-TV-Piraten in Deutschland ist, soll anhand der in den folgenden Tabellen aufgeführten Statistiken dargestellt werden. In den Tabellen werden die Anzahl der erfassten Fälle, deren Aufklärungsrate und die daraus resultierende Anzahl der aufgeklärten Fälle aufgelistet,[371] unter die auch einige Verstöße der Pay-TV-Piraten fallen. Dabei ist zu beachten, dass die erfassten Fälle nicht nur Pay-TV-Piraterie ausmachen. Wie hoch deren Anteil tatsächlich ist, lässt sich anhand der Statistik nicht feststellen.

---

[367] Shepardson, 2002

[368] o.V., o.J.(19)

[369] Janz, 2002

[370] ebenda

[371] Ein bekannt gewordener Fall ist eine rechtswidrige (Straf-)tat nach dem Straftatenkatalog einschließlich der mit Strafe bedrohten Versuche, die auf einer (kriminal-)polizeilichen Anzeige basieren. Ein aufgeklärter Fall ist eine rechtswidrige (Straf-)tat, die aufgrund des (kriminal-)polizeilichen Ermittlungsergebnisses durch einen Tatverdächtigen begangen wurde, der entweder namentlich bekannt ist oder auf frischer Tat ertappt wurde. Die Aufklärungsquote ist das prozentuale Verhältnis von aufgeklärten zu bekanntgewordenen Fällen während des Berichtszeitraumes. Siehe hierzu: o.V., 2004(1).

Für die Berechnung der Entdeckungswahrscheinlichkeit werden die Durchschnittswerte der Jahre 2000 bis 2003 herangezogen (siehe Tabelle 5). 2003 stellte Premiere seine Verschlüsselung um und schätzte die Anzahl der Schwarzseher vor der Umstellung auf über eine Million. Daher soll exemplarisch von einer Million Pay-TV-Piraten in Deutschland ausgegangen werden. Die Entdeckungswahrscheinlichkeit eines Pay-TV-Piraten wird geschätzt, in dem die erfassten bzw. aufgeklärten Fälle eines für die Pay-TV-Piraterie relevanten Gesetzesverstoßes in das Verhältnis zu der geschätzten Zahl der Schwarzseher, hier eine Million, gesetzt wird.

Tabelle 5:
Auszüge aus der polizeilichen Kriminalstatistik

Ausspähen von Daten § 202a StGB			
Jahr	Anzahl erfasster Fälle	Aufklärungsquote in %	Anzahl aufgeklärter Fälle
2000	538	46,1	248
2001	1463	82,6	1208
2002	806	64,4	519
2003	781	57,6	450
∅	897	67,6	606
Computerbetrug nach § 263a StGB[372]			
Jahr	Anzahl erfasster Fälle	Aufklärungsquote in %	Anzahl aufgeklärter Fälle
2000	6600	67	4422
2001	17310	77,9	13484
2002	9531	57	5433
2003	11388	43,2	4920
∅	11207	63	7065

[372] Ohne Debit-Karten-Mißbrauch mit PIN und ohne Mißbrauch von Zugangsberechtigungen von Kommunikationsdiensten.

Datenveränderung, Computersabotage, §§ 303a, 303b StGB			
Jahr	Anzahl erfasster Fälle	Aufklärungsquote in %	Anzahl aufgeklärter Fälle
2000	513	52,6	270
2001	862	45,4	391
2002	1327	38,1	506
2003	1705	39,3	670
∅	1102	41,7	459

Fälschung beweiserheblicher Daten, Täuschung im Rechts-verkehr bei Datenverarbeitung, §§269, 270 StGB			
Jahr	Anzahl erfasster Fälle	Aufklärungsquote in %	Anzahl aufgeklärter Fälle
2000	268	90,3	242
2001	920	95,8	881
2002	228	80,7	184
2003	237	86,5	205
∅	413	91,6	378

Verrat von Betriebs- und Geschäftsgeheimnissen nach § 17 Abs. 2 UWG			
Jahr	Anzahl erfasster Fälle	Aufklärungsquote in %	Anzahl aufgeklärter Fälle
2000	116	94	109
2001	155	93,5	145
2002	132	92,4	122
2003	118	100,8	119
∅	130	95,4	124

Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten			
Jahr	Anzahl erfasster Fälle	Aufklärungsquote in %	Anzahl aufgeklärter Fälle
2000	2198	81,5	1791
2001	8039	84,2	6769
2002	5902	77,1	4550
2003	7003	67	4692
∅	5786	76,9	4451

Quelle: Polizeiliche Kriminalstatistik

Von 2000 bis 2003 wurden durchschnittlich 897 Vergehen nach § 202a StGB, Ausspähen von Daten, erfasst. Bezogen auf die angenommene Tätergruppe von einer Million wurden also gerade einmal 0,0897% aller Fälle erfasst. Aufgeklärt wurden sogar nur 0,0606%. Wegen Computerbetrugs nach § 263a StGB[373] wurden im Durchschnitt 11207 Fälle registriert, dies entspricht 1,1207%. 7065 Fälle oder 0,7065% wurden aufgeklärt. Verstöße gegen §§ 303a und 303b (Datenveränderung und Computersabotage) gab es zwischen 2000 und 2003 im Schnitt 1102mal, aufgeklärt wurden 459 Fälle. Dies entspricht 0,1102% bzw. 0,0459%, bezogen auf eine Million Schwarzseher. 413 Fälle von Fälschung beweiserheblicher Daten (§ 269 StGB) bzw. Täuschung im Rechtsverkehr bei Datenverarbeitung (§ 270 StGB) wurden in dem Zeitraum erfasst, dies entspricht 0,0413% von einer Million. 378 Fälle oder 0,0378% wurden aufgeklärt. Verstöße gegen § 17 Abs. 2 UWG (Verrat von Betriebs- und Geschäftsgeheimnissen) wurden 130mal registriert, dies entspricht 0,013% aller angenommenen Schwarzseher, 124Fälle (Fälle aus vorherigen Jahren werden ebenfalls berücksichtigt) oder 0,0124% wurden aufgeklärt. Bezüglich des Betrugs mit Zugangsberechtigungen zu Kommunikationsdiensten registrierten die Behörden durchschnittlich 5786 Fälle und klärten 4451 auf. Dies entspricht 0,5786% bzw. 0,4451% im Verhältnis zu einer Million Schwarzsehern. Auch Verurteilungen von Pay-TV-Piraten aufgrund der Erschleichung von Leistungen nach § 265a StGB sind selten.[374]

Die hier aufgeführten Vergehen, die entdeckt und registriert wurden, schwanken also zwischen 0,013% und 1,1207%, wenn man von einer gesamten Tätergruppe von einer Million ausgeht. Legt man die aufgeklärten Fälle zugrunde, schwanken die Werte zwischen 0,0124 % und 0,7065%. Setzt man den prozentualen Anteil der erfassten Fälle mit der Entdeckungswahrscheinlichkeit gleich, lässt sich daraus ableiten, dass ein Pay-TV-Pirat am wahrscheinlichsten wegen Computerbetrugs, dessen sich ein Schwarzseher schuldig macht, gefasst worden wäre. Die Entdeckungswahrscheinlichkeit liegt hier bei 1,1207%.

[373] Ohne Debit-Karten-Mißbrauch mit PIN und ohne Mißbrauch von Zugangsberechtigungen von Kommunikationsdiensten

[374] Zingel, 2002

Käme es zu einem Prozess mit einer Verurteilung gegen ihn, wäre der Fall als aufgeklärt einzustufen. Die Wahrscheinlichkeit einer Aufklärung ist ebenfalls beim Computerbetrug am höchsten, mit 0,7065%. Als Strafe drohen ihm nach § 263a StGB bis zu fünf Jahre Haft oder eine Geldstrafe. Um das Risiko in monetären Größen ausdrücken zu können, muss die in Geld bewertete Strafe mit der Entdeckungswahrscheinlichkeit multipliziert werden. Betrüge die Höhe der Geldstrafe beispielsweise 10.000,-€, entstünde für den Schwarzseher ein finanzielles Risiko von 70,65€.[375] Diesen Betrag muss der Schwarzseher zu den übrigen Kosten des Schwarzsehens wie der Beschaffung der benötigten technischen Ausstattung hinzu addieren. Um eine rationale Entscheidung zu treffen, ist diese Summe nun mit den Kosten eines regulären Pay-TV-Zugangs zu vergleichen. Diejenige Zugangsmethode, die die niedrigeren Gesamtkosten verursacht, ist die rationale Wahl.

Käme es tatsächlich zu einer fünfjährigen Gefängnisstrafe, ist als Opportunitätskosten das entgangene (Netto-)Einkommen anzusetzen, das in Freiheit hätte erzielt werden können. Hätte der Täter beispielsweise ein Einkommen von 30.000,-€ pro Jahr, entgingen ihm bei voller Strafverbüßung 150.000,-€. Wird dieser Betrag mit der Entdeckungswahrscheinlichkeit von 0,7065% multipliziert, betrüge das Risiko 1059,75€. Dieser Betrag ist nun wieder zu den übrigen Kosten des illegalen Zugangs zu addieren und anschließend den Gesamtkosten des legalen Zugangs gegenüberzustellen.

Anzumerken ist, dass in den berechneten Entdeckungswahrscheinlichkeiten Fälle enthalten sind, die nicht auf Pay-TV-bezogene Vergehen zurückzuführen sind. Die tatsächliche Entdeckungswahrscheinlichkeit ist daher als weitaus geringer einzuschätzen. Wie unwahrscheinlich eine Verurteilung von Pay-TV-Piraten ist, zeigen folgende Daten: Im Jahr 2002 registrierte die Polizei rund 20.000 Fälle von Computerkriminalität. Nur in 700 Fällen kam es tatsächlich zu einer Verurteilung, davon gerade einmal zwölf aufgrund § 202a StGB.[376] Aufgrund dieser Daten ist daher die Wahrscheinlichkeit für einen Pay-TV-Piraten, entdeckt zu werden, näher bei Null als bei einem Prozent anzusetzen. Nur absolut risikoaverse Zuschauer werden selbst dieses äußerst geringe Risiko meiden und es aus Angst vor Entdeckung und deren Konsequenzen vorziehen, ein legales Abonnement abzuschließen.

Die oben angeführten Zahlen lassen erahnen, wie gering das Risiko für einen Schwarzseher ist, bei seiner illegalen Tätigkeit erwischt zu werden. Dies gilt allerdings nur für den Fall, dass ein Pay-TV-Programm tatsächlich geknackt ist und schwarz empfangen werden kann. Verfügt ein Pay-TV-Sender über eine sichere Verschlüsselung, so wie gegenwärtig z.B. Premiere, gibt es keine Schwarzseher, demnach ist auch die Entdeckungswahrscheinlichkeit gleich Null.

---

[375] 10.000,-€ x 0,7065%

[376] Hankmann, Sprotte, 2004a

4.4. Nicht-monetäre Gründe für die Wahl eines legalen Zugangs

Auch wenn eine Schwarzseh-Lösung die billigere Alternative eines Pay-TV-Zugangs sein sollte, ziehen viele Pay-TV-Abonnenten diese Option nicht in Betracht. Hierfür gibt es eine Reihe von Gründen, die nicht-monetärer Art und damit intangibel sind, sich also einer Quantifizierung und Bewertung entziehen.[377]

Viele Zuschauer möchten sich moralisch anständig und gesetzestreu verhalten und würden bei Nutzung eines illegalen Zugangs von einem schlechten Gewissen geplagt. Oft haben sie auch schlicht Angst vor dem Kontakt mit der Illegalität. Einige Kunden schätzen darüber hinaus den Service, wie z.B. Technik-Hotlines, und die Zuverlässigkeit des Zugangs, die sie nur bei einem regulären Abonnement erhalten. Des weiteren spielen häufig auch Status und Prestige-Denken eine große Rolle. Der Bezug von teurem Pay-TV soll dem Umfeld des Abonnenten finanziellen Wohlstand und einen modernen Lifestyle signalisieren. Tatsächlich hat das Marktforschungsinstitut TNS Infratest herausgefunden, dass Premiere-Abonnenten ein weit überdurchschnittliches Einkommen beziehen.[378]

[377] Brümmerhoff, S. 198

[378] o.V., 2004(2)

5. Handlungsempfehlungen

5.1. Erfolgversprechendes Vorgehen gegen die Pay-TV-Piraterie

Von einer Lösung des Problems audiovisueller Piraterie ist die Branche gegenwärtig weit entfernt. Anstrengungen sollten jedoch grundsätzlich auf drei Ebenen vorgenommen werden: auf produkt- bzw. marktbezogener, auf technologischer und auf juristischer Ebene.[379] Dabei müssen sowohl die Interessen der Pay-TV-Anbieter als auch der -Nachfrager berücksichtigt und so aufeinander abgestimmt werden, dass auf Zuschauerseite das Interesse am Schwarzsehen und gleichzeitig auf Anbieterseite die Kosten für die Pay-TV-Piraterie-Bekämpfung auf ein Minimum reduziert werden können.

Die Gestaltung der Produktangebote sollte eine Anreizstruktur aufweisen, die die Nutzung des legalen Angebotes attraktiv genug macht, damit die Interessenten auf die Erwägung illegaler Alternativen verzichten. Hierbei sollte zum einen das Programmangebot den Kundenwünschen entsprechen, so dass die Zuschauer auch tatsächlich die Zahlungsbereitschaft aufweisen, die sich die Programmanbieter vorstellen. Auch sollten die Anbieter ihr Angebot auf internationaler Ebene prüfen, damit sich potentielle ausländische Zuschauer nicht genötigt fühlen, auf illegale Zugänge zurückgreifen zu müssen, da der Empfang im Inland auf legale Weise, auch bei vorhandener Zahlungsbereitschaft, nicht möglich ist. Auf diese Weise können die Pay-TV-Anbieter sogar noch zusätzliche Abonnenten gewinnen und weitere Einnahmen generieren, die ansonsten den Piraten zufließen.[380] Zum anderen müssen die Preise und das Preis-Leistungsverhältnis des Pay-TV-Programms so gestaltet werden, daß sie illegale Angebote dagegen nicht als überlegen erscheinen lassen. Nur wenn Kosten und Nutzen in einer für den Kunden angemessenen Relation stehen, ist er auch bereit, die geforderten Gebühren zu bezahlen.

Auf technologischer Ebene ist es erforderlich, stets über ein piratensicheres Niveau der Verschlüsselung zu verfügen. Wirksamer Schutz gegen Schwarzseher wird durch die Anwendung insbesondere solcher Verschlüsselungstechniken erreicht, deren illegale Entschlüsselung durch Hacker oder Schwarzseher nur mit unverhältnismäßig hohem Aufwand realisiert werden kann.[381] Eine illegale Decodierung sollte daher so aufwendig und kompliziert sein, dass die Kosten für Schwarzseher höher sind als die regulären Pay-TV-Gebühren.[382] Ist eine Verschlüsselung jedoch mit relativ geringem Aufwand zu umgehen, werden potentielle Kunden von einem teureren legalen Angebot Abstand nehmen und den billigeren illegalen Zugang wählen. Auch der aktuelle Kundenstamm wird erodieren, da einige Abonnenten bei nächster Gelegenheit ihr reguläres Abonnement kündigen und zur billigeren illegalen Alternative wechseln werden.

---

[379] o.V., 2004(10)

[380] Vgl. o.V., 2003(3), S. 23.

[381] Vgl. Dinsel, 1991, S. 10.

[382] Vgl. Haas, 1991, S. 36.

Für den Einsatz von Verschlüsselungssystemen ist immer zu überlegen, ob der Wert der geschützten Inhalte von einem Hacker höher eingeschätzt wird als die Kosten für seinen Angriff.[383] Da auch ein Hacker langfristig mehr Geld verdienen muss als er ausgibt, ist er zum rationalen Handeln gezwungen. Er muss daher die Kosten des Hack-Angriffs mit den späteren Einnahmen aus dem Verkauf seines Wissens bzw. seiner Piratenprodukte abwägen. Seine möglichen Verkaufspreise und damit seine Einnahmen sind nach oben durch die regulären Bezugspreise des Pay-TV-Angebots, in der Regel also durch die Abonnementpreise beschränkt, da kein rational handelnder Konsument mehr Geld für einen illegalen als für einen legalen Zugang ausgeben würde. Durch die limitierte Einnahmenseite ist automatisch auch die Kostenseite beschränkt, dass heißt, besonders aufwendige Angriffe, die hohe Kosten nach sich ziehen, sind für den Hacker nicht lohnenswert und werden daher nicht angewendet. Daher sollten die Verschlüsselungen in erster Linie vor Angriffen schützen, die nur geringen Aufwand erfordern, die Bedrohung durch aufwendige Angriffe ist dagegen deutlich geringer.[384] Allerdings sind auch aufwendige Angriffe nicht ausgeschlossen. Beispielsweise analysieren Hersteller von Verschlüsselungstechnologie durch aufwendiges Reverse Engineering die Anwendungen der Konkurrenz, um deren Funktionsweise zu verstehen und die eigene Sicherheitstechnologie zu verbessern. Die gewonnenen Informationen werden in der Regel geheimgehalten. Dennoch besteht ein Bedrohungspotential, da nicht ausgeschlossen werden kann, dass die Informationen an die Öffentlichkeit gelangen.[385]

Zusätzlich sollte der Einsatz kompatibler Decodier-Technologien erwogen werden. Solange verschiedene Pay-TV-Anbieter unterschiedliche und untereinander nicht kompatible Verschlüsselungen verwenden, müssen Kunden für jede Verschlüsselung einen eigenen Decoder oder ein separates CA-Modul erwerben. Dies ist mit hohen Kosten verbunden und verärgert daher potentielle Kunden. Der Einsatz eines illegalen Moduls ermöglicht dagegen die Decodierung mehrerer Verschlüsselungen und erspart zudem die Abonnementgebühren. Beispielweise ermöglicht die Software Pentacrypt die Entschlüsselung von acht verschiedenen Verschlüsselungssystemen (Irdeto I+II, SECA I+II, NAGRA, VI-ACCESS I+II, x-in-1 Fun[386]). Auch bei den neuen Pay-TV-Angeboten in den deutschen Kabelnetzen ist dieses Problem aktuell. Beispielsweise speist der Betreiber TeleColumbus Programme von KDG und Premiere mit Nagravision-Verschlüsselung und Programmpakete von KabelKiosk in Conax-Verschlüsselung in seine Netze ein, es werden also im gleichen Netz zwei verschiedene Verschlüsselungssysteme verwendet.[387] Für Zuschauer, die auf beide Angebote

---

[383] Vgl. Zimmermann, 1999, S. 57.

[384] Vgl. ebenda, S. 57.

[385] So verklagte im Jahr 2002 Canal Plus Technologies die Firma NDS. Canal Plus beschuldigte NDS, den Canal Plus-Smartcard-Code entschlüsselt und anschließend in das Internet lanciert zu haben. Daraufhin wurde der Markt mit gefälschten Canal Plus-Karten überschwemmt. Siehe hierzu: Röttgers, 2002.

[386] o.V., o.J.(18)

[387] o.V., 2005(4)

zurückgreifen wollen, bleibt derzeit keine andere Möglichkeit, als zwei Decoderboxen anzuschaffen. Ein Anschluss eines CA-Moduls der anderen Verschlüsselung an die CI-Schnittstelle des Decoders ist nicht möglich, da Premiere eine eigene CI-Spezifikation vorschreibt und damit die Grundidee des Common-Interfaces als Standard-Schnittstelle ad absurdum führt.[388] Pay-TV-Anbieter müssen hier aufpassen, dass sie die Kunden mit einer derartigen Politik nicht verärgern und ihre Aufmerksamkeit auf preisgünstigere Piraten-Module lenken.

Auf juristischer Ebene ist es erforderlich, dass alle Bemühungen gegen die Piraterie-Aktivitäten über einen Rückhalt durch entsprechende Gesetzgebung und Strafverfolgungen verfügen. Nur dann kann die abschreckende Wirkung zu einer Reduzierung der illegalen Aktivitäten führen. Hierfür ist auch eine intensive Lobbyarbeit auf nationaler und internationaler Ebene unerlässlich. Diese muss konsequent verfolgt werden, da aufgrund der schnellen technologischen Entwicklung laufend neue Gesetzeslücken entstehen, die so schnell wie möglich geschlossen werden müssen, um den Piraten möglichst wenig Schlupflöcher zu bieten. Sinnvoll ist es z.B., die AEPOC bei ihren Bemühungen zu unterstützen, die Richtlinie 98/84/EG durch einen Zusatz zu erweitern, der auch den privaten Besitz und die private Nutzung von Umgehungsvorrichtungen EU-weit verbietet.[389] Die bisherige Richtlinie beschränkt sich nur auf Handlungen mit kommerziellem Hintergrund[390] und läuft weitgehend leer, da der organisierte Schwarzmarkt seine Geschäftsmethoden entsprechend angepasst hat. Statt gebrauchsfertigen Piraterie-Equipments werden Einzelkomponenten wie Blanko-Smartcards und Programmiergeräte vertrieben, mit denen sich die Schwarzseher in Kombination mit Software aus dem Internet den illegalen Zugang im Schutz ihrer Privatsphäre selbst herstellen können. Auf diese Weise bleiben sowohl die gewerblichen Handlungen der Hersteller und Händler der Technik als auch die Schwarzseher weitgehend unsanktioniert.[391] Eine Ausweitung der Sanktionierung auf den privaten Besitz und die private Nutzung von Umgehungsvorrichtungen wäre ein wichtiger Schritt für die Schwarzseher-Bekämpfung. In einigen nordischen Ländern wird eine derartige Regelung bereits mit Erfolg praktiziert.[392]

Weitergehend sollte auf die Durchsetzung der Anti-Piraterie-Maßnahmen in allen europäischen Ländern und auch darüber hinaus im Rahmen einer paneuropäischen Zusammenarbeit gedrängt werden, damit den Pay-TV-Piraten keine Ausweichmöglichkeiten geboten werden können.[393] In diesem Zusammenhang sollte auch darüber nachgedacht werden, die strafrechtlichen Sanktionen in Form von Freiheits- und/oder Geldstrafen international anzugleichen, um eine einheitlich abschreckende Wirkung gegenüber Pirateriaktivitäten erzielen zu

---

[388] o.V., 2005(3)

[389] o.V., 2003(5)

[390] o.V., 2003(4)

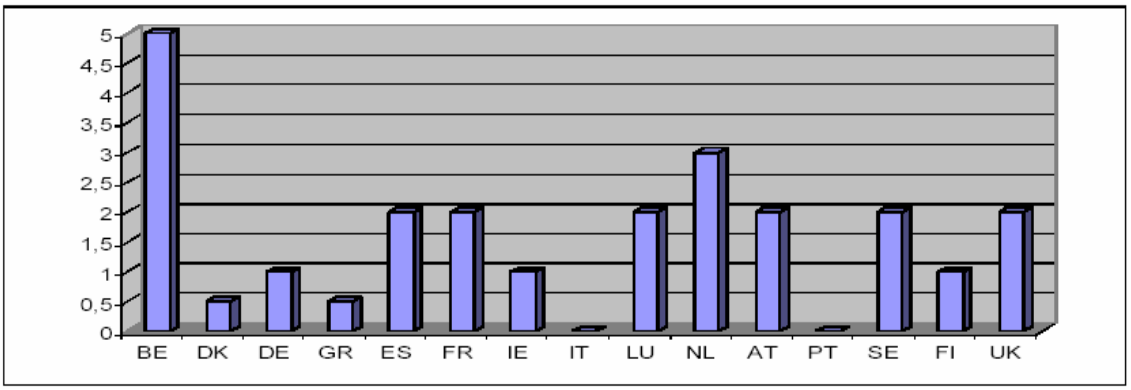
[391] Vgl. o.V., 2003(9), S. 3.

[392] o.V., 2003(3), S. 22

[393] Vgl. o.V., 2003(4).

können. Im Jahr 2003 bestanden hier noch deutliche Unterschiede, wie in Abbildung 13 ersichtlich ist. Während in Belgien die Hauptzuwiderhandlungen mit bis zu fünf Jahren Gefängnis bestraft werden konnten, sahen Italien und Portugal keine derartigen Sanktionen vor.[394]

Abbildung 13:
Maximale Gefängnisstrafe in Jahren für die Hauptzuwiderhandlungen



Quelle: o.V., 2003(3), S. 13.

Auch die Zusammenarbeit mit anderen Organisationen wie z.B. der „World Intellectual Property Organisation“ (WIPO) oder „Motion Picture Association“ (MPA) ist sinnvoll, da sie sich ebenfalls für die Bekämpfung der Piraterie einsetzen und als große Organisationen Einfluss auf Politik, Gesetzgebung und Exekutive hinsichtlich effektiver Bekämpfungsmaßnahmen nehmen können.[395]

Zusätzlich muss versucht werden, das Bewusstseins in der Bevölkerung gegenüber der illegalen Nutzung immaterieller Güter zu verändern und zu schärfen. Die allgemeine Wahrnehmung von Piraterie als Unrecht ist ein Schlüsselkriterium im Kampf gegen die unerlaubte Nutzung von Pay-TV.[396]

5.2. Die optimale Intensität des Schwarzseher-Ausschlusses

Die Intensität der Anstrengungen des Schwarzseher-Ausschlusses durch einen Pay-TV-Anbieter ist dann optimal, wenn die Grenzkosten aller Maßnahmen dem Grenznutzen entsprechen. Eine Ausweitung der Maßnahmen würde dann zu Grenzkosten führen, die höher sind als der dadurch bewirkte Grenznutzen, so dass der Gesamtnutzen vermindert würde. Solange die zusätzlichen Kosten einer Maßnahme jedoch geringer sind als der daraus resultierende Nutzenzuwachs, ist deren Durchführung gesamtnutzensteigernd und damit ökonomisch rational.

Ein vollständiger Ausschluss aller Schwarzseher ist nach dieser Betrachtungsweise nicht notwendig. Sofern es sich bei den Schwarzsehern beispielsweise um eine kleine Gruppe handelt, die mittels einer komplizierten und unpopulären

---

[394] o.V., 2003(3), S. 13

[395] Vgl. o.V., o.J.(10).

[396] o.V., 2004(10)

Zugangseinrichtung Pay-TV illegal empfangen kann und niemals ein reguläres Abonnement abschließen würde, ist deren aufwendige Bekämpfung mittels technischer Maßnahmen und juristischer Verfolgung nicht lohnenswert. Schwarzseher, die auch in Zukunft nicht zu zahlenden Kunden werden möchten, verursachen dem Unternehmen keinen direkten Schaden, da sie eine Leistung nutzen, die ohnehin bereitgestellt wird. Die Grenzkosten für die Ausstrahlung an einen weiteren Empfänger sind Null, da das Fernsehsignal permanent flächendeckend ausgestrahlt wird. Diese Art von Schwarzsehern verursacht dem Pay-TV-Anbieter daher keine direkten Kosten und auch keinen Nutzenentgang in Form von Einnahmeausfällen. Maßnahmen der Bekämpfung würden dann lediglich Kosten verursachen, denen kein oder nur ein verhältnismäßig geringer Nutzen gegenüberstände und so zur Entfernung vom Optimum der Ausschlussintensität beitrüge.

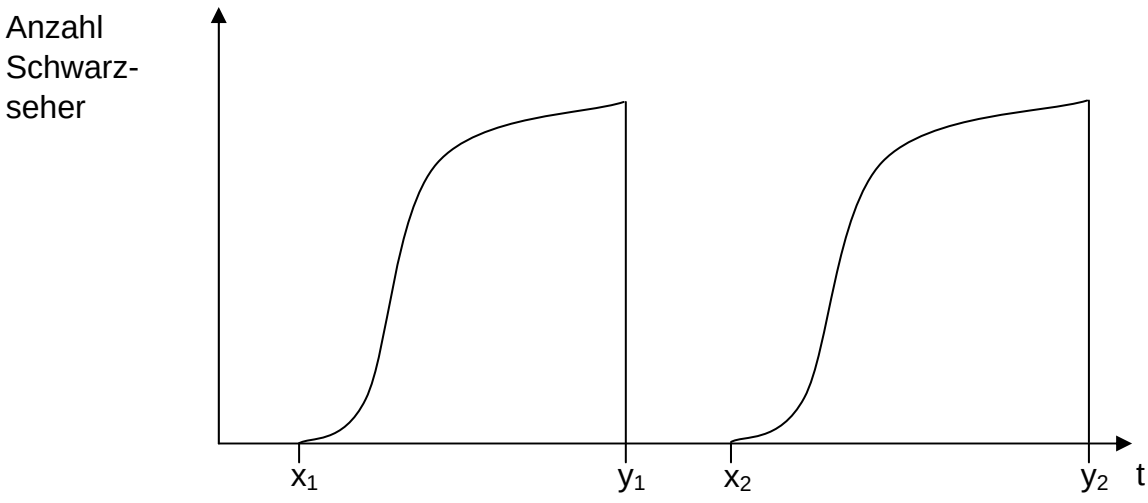
Sind mit Schwarzseher-Aktivitäten jedoch Einnahmeausfälle verbunden, die bei Nicht-Existenz des illegalen Zugangs vermieden würden, können Gegenmaßnahmen ökonomisch sinnvoll sein. Für die Bekämpfung der unternehmensschädigenden Schwarzseher ist immer die Maßnahme zu wählen, die im Verhältnis zum Erfolg die geringsten Kosten verursacht. Eine einfache Änderung des Codes ist technisch nicht besonders aufwendig und daher mit relativ geringen Kosten verbunden. Daher kann eine Codeänderung bereits bei einer geringen Anzahl von grundsätzlich zahlungswilligen Schwarzsehern effizient sein. Kostenintensivere Maßnahmen, etwa eine Verschlüsselungsumstellung, sind dagegen nur dann rational, wenn in deren Folge Einnahmeausfälle in beträchtlicher Höhe vermieden werden können, welche die Kosten der Maßnahme übertreffen.

Wie sich im Verlauf dieser Arbeit herausstellte, verkünden Pay-TV-Anbieter häufig das Ziel des vollständigen Ausschlusses aller Schwarzseher und die Verfolgung jedes Pay-TV-Piraten. Zum einen sind hinter diesen Aussagen öffentlichkeitswirksame und abschreckende Gründe zu vermuten, da eine offizielle Duldung von Schwarzsehern durch einen Sender Imageschäden zur Folge hätte und unter Umständen weitere Zuschauer zum Schwarzsehen verleiten würde. Zum anderen sind die üblichen Schwarzseher-Zugänge, wie illegale Smartcards oder das Beschaffen von Zugangscodes via Internet, weit verbreitet. Zugänge, die nur von wenigen genutzt werden und für einen Sender keinen Schaden bedeuten, gibt es kaum. Damit hat praktisch jede illegale Zugangsmethode signifikante finanzielle Schäden bei den Pay-TV-Anbietern zur Folge. Daher kann es aus Senderperspektive auch wirtschaftlich rational sein, gegen jede Art von Pay-TV-Piraterie vorzugehen und einen vollständigen Ausschluss anzustreben.

6. Pay-TV als temporäres Club-Gut

Durch technische Maßnahmen wie Signal-Verschlüsselungen, Verschlüsselungscodeänderungen oder Systemwechsel versuchen die Pay-TV-Anbieter, Schwarzseher von ihrem Programmangebot auszuschließen. In der Praxis erweisen sich jedoch die technischen Ausschlussmaßnahmen auf Dauer oft als wirkungslos, so dass ein großer Teil der Zuschauer in den Genuss des Programms kommt, auch ohne dafür zu bezahlen. Nach Einführung einer wirksamen Verschlüsselung, die die Zahl der Schwarzseher auf Null reduziert, dauert es eine nicht vorher abschätzbare Zeit, bis eine Umgehungslösung für diese gefunden ist. In der Folgezeit nimmt die Anzahl der Schwarzseher zunächst langsam zu, bis sich herumgesprochen hat, dass ein neuer illegaler Zugang existiert. Ist lediglich ein Update aus dem Internet zu laden, kann aufgrund der einfachen Downloadmöglichkeiten davon ausgegangen werden, dass die Zahl der Schwarzseher wieder sprunghaft ansteigt. Sind neue Smartkarten nötig, müssen diese erst hergestellt, von den Dealern beschafft und verkauft werden. Daher nimmt die Anzahl der Schwarznutzer nicht ganz so schnell zu. Nachdem die routinemäßigen Schwarzseher versorgt sind, wird die Zahl nur noch wenig ansteigen, es kommen dann lediglich weniger ambitionierte Schwarzseher oder einige neue Interessenten hinzu. Sobald eine neue Code- oder Verschlüsselungsänderung erfolgt, bleibt der Fernseher für die Schwarznutzer erneut schwarz und deren Anzahl sinkt abrupt auf Null, bis eine erneute illegale Zugangslösung gefunden wird.

Abbildung 14:
Anzahl der Schwarzseher im Zeitablauf



x_t: Verschlüsselung ist geknackt

y_t: Verwendung einer neuen Verschlüsselung

Quelle: Eigene Darstellung

Das Kriterium der Ausschliessbarkeit zur Unterscheidung von Güterarten kann also offensichtlich nur zum Teil erfüllt werden: In der Zeit, während der eine Verschlüsselung nicht geknackt ist und vollständig vor Schwarzsehern schützt, erfüllt das Gut Pay-TV die Kriterien eines Clubgutes. In diesem Fall liegt neben der Nicht-Rivalität im Konsum auch die Möglichkeit der Ausschliessbarkeit vor. Sobald jedoch durch Hacker eine Umgehungslösung der Ausschlussmechanismen gefunden wird, kann der Ausschluss Nicht-Zahlender nicht mehr durchgesetzt werden. Lediglich für Zuschauer, die aus Kosten-, moralisch-ethischen o.ä. Gründen von illegalen Methoden keinen Gebrauch machen möchten, stellt auch eine geknackte Verschlüsselung eine wirksame Ausschlussmethode dar, so dass hinsichtlich dieser Nutzergruppen nach wie vor Pay-TV als Clubgut kategorisiert werden kann. Bezieht man die Schwarzseher in die Betrachtung jedoch mit ein, so erfüllt Pay-TV temporär, nämlich bei wirksamer Verschlüsselung, die Eigenschaften eines Club-Gutes und temporär, nämlich bei geknackter Verschlüsselung, die eines öffentlichen Gutes. Erfährt der Wert des Gutes Pay-TV durch die Existenz von Schwarzsehern einen Nutzenverlust, beispielsweise für Rezipienten, die Pay-TV aus Statusgründen abonnieren und sich dann nicht mehr von Schwarzsehern geringeren Wohlstandes abheben können, entsteht eine Konsumrivalität. Dadurch würde das Gut Pay-TV in Richtung eines Allmendegutes tendieren, welches sich durch Rivalität im Konsum bei gleichzeitiger Nicht-Ausschliessbarkeit auszeichnet. Eine eindeutige Zuordnung zu einer Güterkategorie gemäß dem dichotomen Betrachtungsschema aus Kapitel 2.4.1. greift daher in praxi zu kurz.

Auch bei der Diffundierung der Software für den illegalen Zugang zeigt sich ein interessantes Phänomen: Hacker, die die Umgehungssoftware entwickeln, stellen diese für sämtliche Nutzer kostenlos im Internet bereit. Aufgrund der einfachen und schnellen Downloadmöglichkeiten von jedem beliebigen Internetzugang aus wird diese Software zu einem Kollektivgut, für die die Nutzer keine Gegenleistung erbringen müssen und der Entwickler nicht in Relation zu seinen erbrachten Aufwendungen und Anstrengungen entlohnt wird. Das Grundschema des ökonomischen Verhaltens im nicht-öffentlichen Bereich, nämlich das Erhalten einer Leistung gegen Erbringung einer äquivalenten Gegenleistung, ist hier für das Verhältnis zwischen Softwareentwickler und Softwarenutzer nicht mehr anwendbar. Der Hacker kann zunächst lediglich einen individuellen Nutzwert aus in Hackerkreisen erlangtem Ruhm für die erfolgreiche Entschlüsselung ziehen. Bei Erreichen einer gewissen „Reputation“ kann der Hacker jedoch, wie bereits erwähnt, auf die Erlangung einer lukrativen Tätigkeit in der (Software-)Industrie hoffen, so dass der zuvor getätigte Aufwand als Investition in seine Zukunft gesehen werden kann, von dem zusätzlich Tausende Schwarzseher profitieren.

7. Zusammenfassung

In der vorliegenden Diplomarbeit wurde das Schwarzseher-Problem im Bereich des Pay-TV analysiert. Als betriebswirtschaftliche Arbeit wurde der Schwerpunkt der Analyse auf die Kosten-Nutzen-Betrachtung gelegt. Dabei wurde das Problem aus zwei Betrachtungswinkeln untersucht: zum einen aus der Perspektive der Pay-TV-Anbieter, zum anderen aus der Sicht der Schwarzseher.

Zunächst wurde sich dem Problem aus der Sicht der Pay-TV-Anbieter genähert. Nach der Einführung in die Problematik der Pay-TV-Piraterie wurden deren ökonomische Auswirkungen dargestellt. Anschließend wurden die Ausschlussmethode des Pay-TV, die Verschlüsselung, erläutert und die damit verbundenen Kosten sowie deren Nutzen betrachtet. Im weiteren Verlauf wurden dann Kosten und Nutzen der Bekämpfungsmethoden der Pay-TV-Piraterie, die auf technischer und juristischer Ebene vorgenommen werden, analysiert.

Im Anschluss daran wurden Kosten und Nutzen aus Sicht der Pay-TV-Piraten, zu denen neben den Schwarzsehern auch die Hacker und Dealer der Piraterie-Technik gehören, herausgearbeitet. Dabei wurde nicht nur auf die benötigte technische Ausstattung der Schwarzseher eingegangen, auch die technischen und juristischen Risiken, die sich aus der Pay-TV-Piraterie ergeben, fanden Berücksichtigung.

Aus den während des Verlaufs der Untersuchung gewonnenen Erkenntnissen wurden daraufhin Handlungsempfehlungen für die zukünftige Bekämpfung der Pay-TV-Piraterie abgeleitet. Zusätzlich wurde die optimale Intensität der Anstrengungen des Ausschlusses von Schwarzsehern durch Pay-TV-Anbieter erörtert.

Abschließend wurde gezeigt, dass eine eindeutige Zuordnung des Gutes Pay-TV zu der Güterart eines Clubgutes nicht unbedingt möglich ist, da das Ausschlusskriterium nicht immer erfüllt werden kann.

Während der Analyse stellte sich heraus, dass Piraterie beim Pay-TV nach wie vor ein aktuelles Problem ist und sich mittlerweile zu einem Milliarden-Markt entwickelt hat. Für die Pay-TV-Anbieter ist dies mit erheblichen finanziellen Verlusten verbunden, die sogar existenzbedrohend sein können. Die Bekämpfung der Piraterie bedeutet eine große Herausforderung. Für den Schutz vor unberechtigtem Zugang zu den kostenpflichtigen Programmen und für die Bekämpfung von Pay-TV-Piraten entstehen den Sendern hohe Kosten. Wie in der vorliegenden Arbeit gezeigt wurde, ist es notwendig, dass die angewendeten Maßnahmen zur Schwarzseher-Vermeidung stets ökonomisch rationalen Anforderungen genügen müssen, um die Finanzkraft der betroffenen Pay-TV-Unternehmen nicht noch zusätzlich zu den durch Piraten angerichteten Schäden zu schwächen. Jede durchgeführte Maßnahme gegen Pay-TV-Piraterie sollte daher einen höheren (monetären) Nutzen stiften als sie an Kosten verursacht. In der Arbeit wird jedoch auch herausgestellt, dass mit der Ermittlung von Kosten und Nutzen Schwierigkeiten verbunden sein können.

Aufgrund des begrenzten Umfangs dieser Diplomarbeit konnte nicht jeder angesprochene Aspekt erschöpfend untersucht werden. Es wurden jedoch die wichtigsten Ansatzpunkte der gegenwärtigen Schwarzseher-Problematik aus betriebswirtschaftlicher Sicht dargestellt. Da das Schwarzseher-Problem beim Pay-TV auch in absehbarer Zukunft von hoher Relevanz sein wird, sind weitergehende und vertiefende Arbeiten lohnenswert.

Anhang

Tabelle 6:
Ausgewählte, in Europa über Satellit ausstrahlende Pay-TV-Anbieter

Hauptmarkt	Pay-TV-Anbieter
Belgien	AB Sat
Dänemark	Canal Digital
	Danmark 1&2
	Viasat
Deutschland	Premiere
Finnland	TV Finland
	Viasat
Frankreich	AB Sat
	Canal Satellite France
	Globecast
	TPS
Griechenland	Alpha Digital
	Nova
Großbritannien	BBC Prime
	BskyB
	Globecast
	God Digital
	MTV Networks
	Sky Digital
Italien	RAI
	Sky Italia
	Stream
	Telespazio
	Tele+ Digitale
Kroatien	HRT
Luxemburg	AB Sat
Niederlande	Canal Digitaal Satelliet

Hauptmarkt	Pay-TV-Anbieter
Norwegen	Canal Digital
	NRK International
Österreich	ORF
	Premiere
Polen	Cyfra+
	Polsat Cyfrowy
	TVN
	TV Polonia
	Wizja TV
Portugal	TV Cabo
Rumänien	RR Satellite Communications
Rußland	NTV Mir
	RTV International
Schweden	Canal Digital
	SVT
	Viasat
Serbien	TV Pink
	Pink Plus / Globecast
Slowakei	UPC Direct
Slowenien	RTV Slovenija
	SLO
Spanien	Digital+
	RTVE
Tschechische Republik	UPC Direct
Türkei	Cine+ Digital
	DigiFunClub
	Digiturk
	Dogus Grubu
Ungarn	Antenna Hungaria
	UPC Direct
Zypern	Alpha Digital
	Nova

Tabelle 7:
Gehackte Pay-TV-Sender in Europa
(Stand: November 2004)

Pay-TV-Anbieter	Land	Verschlüsselung
AB-Sat	Frankreich	Seca/Mediaguard
Canal Digitaal Satelliet	Niederlande	Irdeto
Canal Satellite France	Frankreich	Seca/Mediaguard
Digital+	Spanien	Seca/Mediaguard
MTV Networks	England	Cryptoworks
ORF	Österreich	Cryptoworks
Sky Italia	Italien	Seca/Mediaguard
TPS	Frankreich	Seca/Mediaguard

Die Tabelle zeigt eine Momentaufnahme. Durch Änderungen des Verschlüsselungscodes können einige Sender wieder „dunkel“, also für Schwarzseher nicht empfangbar sein. Ebenso können mit der Zeit weitere Programme gehackt werden, in der Hacker-Sprache als „hell“ bezeichnet. Nicht immer kann jedoch bei gehackten Programmen das gesamte Programm-Bouquet schwarz empfangen werden.

Quelle: Hankmann, Sprotte, 2004d

Tabelle 8:
Hacker-Vokabeln

Hacker-Sprache	Bedeutung
aufbohren	Ändern der Firmware einer Smartcard oder Set-Top-Box
Blocker	Blocker verhindern, daß ECM-Datenpakete zu einer ge hackten Smartcard durchgelassen werden
böses ECM	Die ECM-Daten stimmen nicht mit denen der illegalen Smartcard überein, daher wird die Karte abgeschaltet
Cardsharing	Über einen Internet-Server werden die Daten einer Original-Smartcard an angeschlossene Nutzer verteilt, die das Programm dann illegal empfangen können
Dumpen	Ändern der Version einer Smartcard
dunkel	Verschlüsseltes Programm, das nicht geknackt ist
EMU	Abkürzung für Emulation; Software, mit der verschlüsselte Programme freigeschaltet werden können
funzen	funktionieren
hell	verschlüsseltes Programm, das geknackt ist
Keys	Verschlüsselungscodes
Killen	Vorgang des Hackens einer Smartcard
Loggen	Abhören und Auswerten der geschützten Daten einer Smartcard
MOSC	Modified Original Smartcard; Bezeichnung für die Smartcard-Hacker-Szene
Nullen	Originaldaten einer Smartcard werden komplett gelöscht
Patchen	Ändern der Software einer Original-Smartcard
Prob	Problem
Progger	Gerät, mit dem Blanko-Smartcards beschrieben werden können
Soft	Abkürzung für Software

Quelle: Hankmann, Sprotte, 2004c, S. 86.

Literaturverzeichnis

Abel, John D.: Current Pay-TV Programmers: Their Experiences and Strategies for Launching Systems in the United States, in: Pay-TV - Technische Grundlagen, Erfahrungen, Wirtschaftlichkeit und Zukunftsaspekte, hrsg. vom: Verband privater Rundfunk und Telekommunikation (VPRT), Bonn 1991

Adamcewski, David: DirecTV geht gegen Schwarzseher vor, in Internet: http://www.heise.de/newsticker/meldung/25968, 22.03.2002, Stand: 05.03.2005

Bär, Wolfgang, Hoffmann, Helmut: Das Zugangskontrolldiensteschutz-Gesetz, in: Multimedia und Recht, Nr. 10, 2002, S. 654-658

Bahr, Martin: Entschlüsselung von Pay-TV / Zugangskontrolldienste-Gesetz / ZKDSG, in Internet: http://www.dr-bahr.com/faq/faq_rechtderneuenmedien-.php#RechtderNeuenMedien_id6, o.J., Stand: 20.01.2005

Becker, Udo.: Existenzgrundlagen öffentlich-rechtlicher und privater Rundfunkveranstalter nach dem Rundfunkstaatsvertrag, Baden-Baden 1992

Bechtold, Stefan: Schutz und Identifizierung durch technische Schutzmaßnahmen, in: Handbuch Multimedia-Recht, hrsg. von: Thomas Hoeren, Ulrich Sieber, 9. Ergänzungslieferung April 2004, München, 2004, S. 1-66

Blum, Ulrich: Volkswirtschaftslehre: Studienhandbuch, 2. überarb. Auflage, München u.a. 1994

Brümmerhoff, Dieter: Finanzwissenschaft, 8. Auflage, München 2001

Buschendorf, Anja, 2005a: ProSiebenSat.1 Welt startet heute in den USA, in Internet: http://www.digitalfernsehen.de/news/news_23137.html, 22.02.2005, Stand: 23.02.2005

Buschendorf, Anja, 2005b: Humax: Kooperation mit US-Pay-TV-Marktführer, in Internet: http://www.digitalfernsehen.de/news/news_23943.html, 08.03.2005, Stand: 10.03.2005

Busse, Caspar-Peter: Pay-TV fasziniert auch Pro Sieben Sat1, in: Handelsblatt, Nr. 38, 23.02.2005, S. 17

Clover, Julian: European Digital Pay TV Revenues. Market Assessment and forecasts to 2006, in Internet: http://www.markt-studie.de/ueberstudie-15_2748.html#mehrinfos, Januar 2004, Stand: 16.01.2005

Dietl, Helmut, Franck, Egon: Free-TV, Abo-TV, Pay per View-TV – Organisationsformen des privaten Fernsehangebots als Arrangements zur Vermarktung von Unterhaltung, Freiberger Arbeitspapiere, Nr. 22, hrsg. von der Technischen Universität Bergakademie Freiberg, o.O. 1999

Dinsel, Siegfried: Die Technik der Verschlüsselung von Fernsehsignalen, in: Pay-TV - Technische Grundlagen, Erfahrungen, Wirtschaftlichkeit und Zukunftsaspekte, hrsg. von: Verband privater Rundfunk und Telekommunikation (VPRT), Bonn 1991

Fiutak, Martin: TV-Sender Premiere wählt neue Verschlüsselung, in Internet: www.zdnet.de/news/business/0,39023142,39116599,00.htm, 17.10.2003, Stand: 20.10.2004

Freyer, Ulrich: Digitaler Rundfunk, in Internet: http://www.alm.de/digi.htm, o.J., Stand: 16.01.2005

Goedecke, Stefan, Hofmeir, Stefan, 2003a: Höchste Sicherheit gegen Hacker, in: Digitalfernsehen, Nr. 8, 2003, S. 12-13

Goedecke, Stefan, Hofmeir, Stefan, 2003b: Nepper, Schlepper, Bauernfänger, in: Digitalfernsehen, Nr. 11, 2003, S. 36-39

Goedecke, Stefan, Hofmeir, Stefan, 2003c: Schwarzseher aufgepaßt!, in: Digitalfernsehen, Nr. 11, 2003, S. 22-24

Goedecke, Stefan, Hofmeir, Stefan, 2003d: So wehrt sich Premiere gegen die Piraterie, in: Digitalfernsehen, Nr. 11, 2003, S. 26

Große Peclum, Marie-Luise: Europäische Perspektiven, in: Pay-TV – Technische Grundlagen, Erfahrungen, Wirtschaftlichkeit und Zukunftsaspekte, hrsg. von: Verband privater Rundfunk und Telekommunikation (VPRT), Bonn 1991

Haas, Eckart: Wirtschaftliche Kenndaten und Auswahlkriterien von Pay-TV-Systemen, in: Pay-TV - Technische Grundlagen, Erfahrungen, Wirtschaftlichkeit und Zukunftsaspekte, hrsg. von: Verband privater Rundfunk und Telekommunikation (VPRT), Bonn 1991

Hagedorn, Stefan: Transponder NEWS, 12./13.10.02, in Internet: http://archiv.transponder-news.de/sat-stefan-2002/140.html, 13.10.2002, Stand: 3.12.2004

Hagedorn, Stefan, 2004a: Code wechsle dich!, in: Digitalfernsehen, Nr. 11, 2004, S. 20-21

Hagedorn, Stefan, 2004b: Die Verschlüsselungssysteme, in: Digitalfernsehen, Nr. 11, 2004, S. 20

Hankmann, Marc, Sprotte, Susanne, 2004a: Ausspähen von Daten, in: Digitalfernsehen, Nr. 11, 2004, S. 88

Hankmann, Marc, Sprotte, Susanne, 2004b: Das benutzt der Hacker, in: Digitalfernsehen, Nr. 11, 2004, S. 89

Hankmann, Marc, Sprotte, Susanne, 2004c: Die Sprache der Hacker, in: Digitalfernsehen, Nr. 11, 2004, S. 86-89

Hankmann, Marc, Sprotte, Susanne, 2004d: Pay-TV – Das sieht der Hacker, in: Digitalfernsehen, Nr. 11, 2004, S. 87

Hankmann, Marc, Sprotte, Susanne, 2004e: „Piratenkarten werden noch lange Wunschtraum bleiben“, Interview mit dem Leiter von Premiere E-Security, Michael Söllner, in: Digitalfernsehen, Nr. 11, 2004, S. 87

Hankmann, Marc, Sprotte, Susanne, 2004f: Zerstörte Box durch Hacker-Abzocke, in Digitalfernsehen, Nr. 11, 2004, S. 89

Hansmeyer, Karl-Heinrich, Kops, Manfred: Rundfunkprogramme als Klubgüter, Arbeitspapiere des Instituts für Rundfunkökonomie an der Universität zu Köln, Nr. 91, Köln 1998

Heinrich, Jürgen: Medienökonomie, Band 2: Hörfunk und Fernsehen, Opladen/-Wiesbaden 1999

Herres, Torsten: Verschlüsselungs-Premiere, in: Digitalfernsehen, Nr. 5, 2003, S. 12-13

Hofmeir, Stefan: Premiere, Pay-TV und Piraten, in: Funkschau, Jg. 66, Nr. 3, 1994, S. 22-29

Hofmeir, Stefan, 2003a: Erste Erfahrung mit dem ZKDSG-Gesetz, in: Digitalfernsehen, Nr. 5, 2003, S. 16-17

Hofmeir, Stefan, 2003b: Keine Chance für Piraten, in: Digitalfernsehen, Nr. 5, 2003, S. 16

Hofmeir, Stefan, 2005a: „Bei uns gibt es keine Wartezeiten mehr“, Interview mit dem Geschäftsführer der TESC, Wilfried Urner, in Digitalfernsehen, Nr. 3, 2005, S. 23

Hofmeir, Stefan, 2005b: So werden Premiere-Receiver zertifiziert, in: Digitalfernsehen, Nr. 3, 2005, S. 22-23

Hofmeir, Stefan, Herres, Torsten: Spezielle Nagravision, in: Digitalfernsehen, Nr. 5, 2003, S. 7

Hunsel, Lothar: Premiere - Das neue deutschsprachige Pay-TV-Programm, in: Pay-TV - Technische Grundlagen, Erfahrungen, Wirtschaftlichkeit und Zukunftsaspekte, hrsg. von: Verband privater Rundfunk und Telekommunikation (VPRT), Bonn 1991

Jakobs, Hans-Jürgen: d-Box: Die Chaos-Kiste, in: Der Spiegel, Nr. 52, 2000, Seite 106-108, in: Internet: http://t-off.khd-research.net/Spiegel/27.html, Stand: 04.12.2004

Janz, Nicole: Ende der Schonzeit, in Internet: http://www.lostinmusic.de/lim/-news/archiv_2002/Ende%20der%20Schonzeit.htm, 13.09.2002, Stand: 25.12.2004

Karepin, R.: Pay-TV faßt allmählich in Deutschland Fuß, in: Horizont, Nr. 42, 1993, S. 61, zitiert nach: Pagenstedt, Georg: Strategische Planung für Anbieter von Abonnementfernsehen, Diss., Universität zu Köln 1995

Koschnik, Wolfgang J.: Pay-TV, in Internet: http://medialine.focus.de/PM1D/-PM1DB/PM1DBF/pm1dbf_d.htm?snr=4240, Stand: 19.10.2004

Krüger, Eva: AW: Fragebogen zum Thema Pay-TV-Piraterie, Eva.Krueger@-ish.com, Absendedatum der E-Mail: 16.12.2004

Laga, Gerhard: Rechtliche Beurteilung von technischen Schutzmaßnahmen, in Internet: http://www.laga.at/Doks/Tech-Schutz.pdf, 06.09.1999, Stand: 02.02.2005

Lenhardt, Helmut: Einführung, in: Pay-TV - Technische Grundlagen, Erfahrungen, Wirtschaftlichkeit und Zukunftsaspekte, hrsg. von: Verband privater Rundfunk und Telekommunikation (VPRT), Bonn 1991

Liebert, Frank: ohne Titel, in Internet: http://www1.digitalfernsehen.de/katalog/-stb.php?betacryptNav=1, Stand: 19.10.2004

Lievaart, N.: Piracy, in Internet: http://www.irdetoaccess.com/docs/ia_on_piracy-.pdf, 2001, Stand: 02.11.2004

Linow, Oliver: CAT: Schlüsseldienst für „berechtigten“ Fernsehgenus, in: Digitalfernsehen, Nr.12, 2004, S. 92

Mankiw, N. Gregory: Grundzüge der Volkswirtschaftslehre, 3. Aufl., Stuttgart 2004

McCarthy, Arlene, Fourtou, Janelly, Manders, Toine, Echerer, Mercedes, Arburua, Marcelino Oeja: Written declaration on the fight against piracy and counterfeiting in the enlarged EU, in Internet: http://www.europarl.eu.int/-Declaration/document/2003/P5_DCL(2003)0005/P5_DCL(2003)0005_EN-.doc, 26.03.2003, Stand: 23.12.2004

Meyer, Thomas, Sprotte, Susanne, 2003a: CA-Module und Preise, in: Digitalfernsehen, Nr. 11, 2003, S. 120

Meyer, Thomas, Sprotte, Susanne, 2003b: Flickenteppich oder Fernsehen ohne Grenzen?, in: Digitalfernsehen, Nr. 11, 2003, S. 118-122

Michaelsen, Lars: Marktstrategien für Pay-per-view-Veranstalter, Arbeitspapiere des Instituts für Rundfunkökonomie an der Universität zu Köln, Nr. 67, Köln 1996

Mitiu, Chris: SECA - Société Européenne de Controle d' Access, in Internet: http://www.satlex.de/de/dictionary-term_SECA.html, Stand: 26.11.2004

Müller, Dietmar: Premiere will Schwarzseher zu Abonnenten machen, in Internet: http://www.zdnet.de/news/tkomm/0,39023151,2138948,00.htm, 1.9.2003, Stand: 05.10.2004

Nickles, Michael: 1000 TV-Programme für 200 Euro, in Internet: http://www.nickles.de/c/s/30-0013-198-1.htm, 20.2.2002, Stand: 25.12.2004

o.V., 1999: Einführung in die Kryptographie, in: Einführung in die Kryptographie, in Internet: www.rzbd.fh-hamburg.de/ftp/files/kryptografie.pdf, 1999, Stand: 08.12.2004

o.V., 2001a: Pay-TV-Sender hackt Hacker, in Internet: http://www.rp-online.de/-news/multimedia/tv/hacker_gehackt.html, 06.02.2005, Stand: 02.03.2005

o.V., 2001b: Pay-TV Hacker geschnappt, in Internet: http://www.rp-online.de/-news/multimedia/allgemein/hacker_geschnappt.html, 13.02.2001, Stand: 05.12.2004

o.V., 2002(1): Premiere: Schwarzseher ausgesperrt, in Internet: http://www.-tkv.com/news.php?sprache=deu, 19.03.2002, Stand: 03.12.2004

o.V., 2002(2): Premiere schließt Sicherheitslücke, in Internet: http://www.tkv.-com/news.php?sprache=deu, 20.03.2002, Stand: 03.12.2004

o.V., 2002(3): Hacker knacken weiter hemmungslos Premiere, in Internet: http://www.dvb-technik.de/modules.php?name=News&file=article&sid=84, 08.04.2002, Stand: 10.12.2004

o.V., 2002(4): New Media Markets, 31.05.2002, S. 6, zitiert nach: o.V., 2003(3): Rechtlicher Schutz elektronischer Bezahldienste, S. 20, in Internet: http://-europa.eu.int/eur-lex/de/com/rpt/2003/com2003_0198de01.pdf, 24.04.2003, Stand: 12.02.2005

o.V., 2002(5): Conax distanziert sich von Hacker-Modulen, in Internet: http://-www.tkv.com/news.php?sprache=deu, 02.08.2002, Stand: 03.12.2004

o.V., 2002(6): Polizeischlag gegen illegalen Handel mit Decodern und Smart-cards, in Internet: http://www.tkv.com/news.php?sprache=deu, 02.08.2002, Stand: 03.12.2004

o.V., 2002(7): Premiere-Hacker verurteilt, in Internet: http://www.tkv.com/-news.php?sprache=deu, 02.08.2002, Stand: 03.12.2004

o.V., 2002(8): Magic Module soll via Satellit deaktiviert werden, in Internet: http://www.tkv.com/news.php?sprache=deu, 13.08.2002, Stand: 03,12,2004

o.V., 2002(9): SCM appelliert an Händler wegen Pay-TV-Piraterie, in Internet: http://www.tkv.com/news.php?sprache=deu, 21.08.2002, Stand: 03.12.2004

o.V., 2002(10): Razzia gegen Piraterie, in Internet: http://www.infosat.de/Mel-dungen/?msgID=7308, 30.08.2002, Stand: 20.12.2004

o.V., 2002(11): Kofler will bis zu 1,5 Millionen Schwarzseher als Kunden ge-winnen, in Internet: http://www.tkv.com/news.php?sprache=deu, 14.09.2002, Stand: 03.12.2004

o.V., 2002(12): Verkaufsstopp für Magic Module, in: Internet: http://www.tkv.-com/news.php?sprache=deu, 20.09.2002, Stand: 03.12.2004

o.V., 2002(13): Common-Interface: Was ist legal, was nicht?, in Internet: http://-www.tkv.com /news.php?sprache=deu, 27.09.2002, Stand: 03.12.2004

o.V., 2002(14): Smart-Card-Tausch sorgt für Abo-Anstieg, in Internet: http://-www.tkv.com/news.php?sprache=deu, 14.10.2002, Stand: 03.12.2004

o.V., 2002(15): Pay-TV-Hehler zu Freiheitsstrafe verurteilt, in Internet: http://-www.tkv.com/news.php?sprache=deu, 16.10.2002, Stand: 03.12.2004

o.V., 2002(16): Piracy Threat for Pay-TV Services, in Internet: http:// groups.google.de/groups?q=pay+tv+hack&start=40&hl=de&lr=&selm=r6uI9.5 386%24B03.11888%40news-server.bigpond.net.au&rnum=41, 08.12.2002, Stand: 05.12.2005

o.V., 2003(1): Pay-TV-Piraterie ist strafbar, in Internet: http://www2.digitalfern-sehen.de/Home/1050985765/2003_2_23_1045996970/copy_of_copy2_of_ 1050985985, 23.02.2003 Stand: 11.11.2004

o.V., 2003(2): Das neue Premiere, in Internet: http://www.premiere.de/content/-download/kennzahlen-250203.final.pdf, 26.02.2003, Stand: 31.12.2004

o.V., 2003(3): Rechtlicher Schutz elektronischer Bezahldienste, in Internet: http://europa.eu.int/eur-lex/de/com/rpt/2003/com2003_0198de01.pdf, 24.04.2003, Stand: 12.02.2005

o.V., 2003(4): Electronic piracy must be stamped out to protect Europe's competitiveness, says Commission report, in Internet: http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/03/583&format=HTML&aged=1&language=EN&guiLanguage=en, 29.04.2003, Stand: 22.12.2004

o.V., 2003(5): AEPOC welcomes E.U. Commission's explicit analysis of threats to European media business and proposes further steps against piracy of electronic pay-services, in Internet: http://www.aepoc.org/press_service/pr_070503.html, 07.05.2003, Stand: 21.12.2004

o.V., 2003(6): OLG Frankfurt, Urteil vom 05.06.2003 Az.: 6 U 7/03(Magic Modul), in Internet: http://www.beckmannundnorda.de/magicmodule.html, 05.06.2003, Stand: 25.12.2004

o.V., 2003(7): Premiere gelingt wichtiger juristischer Schlag gegen Digital-Piraterie, in Internet: http://www.premiere.de/content/43463.jsp, 26.08.2003, Stand: 15.11.2004

o.V., 2003(8): 1st AEPOC European Anti-Piracy Symposium sets the course in the fight against piracy of audiovisual services, in Internet: http://www.-aepoc.org/press_service/pr_131003.html, 13.10.2003, Stand: 21.12.2004

o.V., 2003(9): Fragen zur weiteren Reform des Urheberrechts in der Informationsgesellschaft („Zweiter Korb“), in Internet: http://www.bvdw.org/de/data/doc/2100_001_035_stellungnahme_fragenkatalog_031030_v8_endg.doc, 30.10.2003, Stand: 05.02.2005

o.V., 2003(10): Zappenduster für Schwarzseher: Premiere gibt es seit heute nur noch legal, in Internet: http://www.info.premiere.de/inhalt/de/medienzentrum_news_30_10_2003.jsp, 30.10.2003, Stand: 22.12.2004

o.V., 2004(1): Begriffserläuterungen, in Internet: http://www.bka.de/pks/-pks2003/c.pdf, 2004, Stand: 27.12.2004

o.V., 2004(2): Die Abonnenten im Fokus, in Internet: http://www.media.-premiere.de/download/Soziodemografie.pdf, 2004, Stand: 25.02.2005

o.V., 2004(3): Partner & Mitgliedschaften, in Internet: http://www.humax-digital-.de/abouthumax/partnersnmemberships.asp, 2004, Stand: 05.12.2004

o.V., 2004(4): Digital+ wechselt Verschlüsselung, in Internet: http://www.tg-satellit.de/index.php?shownews=75, 24.03.2004, Stand: 18.10.2004

o.V., 2004(5): AEPOC targets piracy of audiovisual services in the enlarged E.U., in Internet: http://www.aepoc.org/press_service/pr_160404.html, 16.04.2004, Stand: 22.12.2004

o.V., 2004(6): Owning a pay-TV descrambler shouldn't get you sued, in Internet: http://groups.google.de/groups?q=pay+tv+hack&start=10&hl=de&lr=&selm=3d6ef8e5.0406182334.349d054a%40posting.google.com&rnum=11, 18.06.2004, Stand: 05.01.2005

o.V., 2004(7): Bundeskartellamt beabsichtigt Untersagung der Übernahme von ish, KBW und iesy durch KDG, in Internet: http://www.bundeskartellamt.de/wDeutsch/aktuelles/presse /2004_08_24.shtml, 24.08.2004, Stand: 18.12.2004

o.V., 2004(8): AEPOC Workshop in Vicenza denounced piracy of audiovisual services, in Internet: http://www.aepoc.org/press_service /pr_071004.html, 07.10.2004, Stand: 22.12.2004

o.V., 2004(9): Ausstattung privater Haushalte mit Informations- und Kommunikationstechnik in Deutschland, in Internet: http://www.destatis.de/basis/d/evs/budtab2.php, 15.10.2004, Stand: 04.01.2005

o.V., 2004(10): 2nd AEPOC European Anti-Piracy Symposium: Media industry in agreement on main approaches to piracy of audiovisual services, in Internet: http://www.aepoc.org/press_service/pr_271004_2.html, 27.10.2004, Stand: 22. 12. 2004

o.V., 2004(11): Premiere-Bestellformular, Stand: November 2004

o.V., 2004(12): Premiere-Werbeprospekt, Stand: November 2004

o.V., 2004(13): AEPOC expects piracy problem to worsen 2005 and after, in Internet: http://www.aepoc.org/press_service/pr_211204.html, 21.12.2004, Stand: 23.12.2004

o.V., 2005(1): Zahlen, Daten, Fakten, in Internet: http://info.premiere.de/inhalt/de/unternehmen_kennzahlen_start.jsp, 2005, Stand: 25.02.2005

o.V., 2005(2): Eutelsat und DNMG arbeiten bei der Vermarktung deutscher digitaler Pay-TV-Programme zusammen, in Internet: http://www.infosat.info/Meldungen/?srID=4&msgID=13816, 16.02.2005, Stand: 19.02.2005

o.V., 2005(3): Was bedeutet neue KDG Boxenstrategie?, in Internet: http://www.infosat.de/Meldungen/?msgID=13850, 17.02.2005, Stand: 01.03.2005

o.V., 2005(4): Digitalboxen mit zwei CA-Systemen machen Sinn, in Internet: http://www.infosat.de/Meldungen/?msgID=14181, 10.03.2005, Stand: 11.03.2005

o.V., o.J.(1): Alle aktuellen Angebote im Überblick unter: http://www.premiere.de/content/Abonnieren_pakete_und_preise_Start.jsp?wkz=TO136I4, o.J., Stand: 13. 10.2004

o.V., o.J.(2): American Forces Radio and Television Service, in Internet: http://www.afrts.osd.mil/, o.J., Stand: 26.11.2004

o.V., o.J.(3): Auftrag für Ish Digital TV, in Internet: http://www.ish.de/Generic/Auftrag_Plus_TV_kurz,0.pdf, o.J., Stand: 01.12.2004

o.V., o.J.(4): By-Laws, in Internet: http://www.aepoc.org/about_aepoc/by-laws-.htm, o.J., Stand: 08.02.2005

o.V., o.J.(5): Die Smartcard – Ihr Schlüssel zum Premiere Programm, in Internet: http://www.premiere.de/content/technik_hilfe_smartcard.jsp, o.J., Stand: 19.12.2004

o.V., o.J.(6): Digitale Angebote, in Internet: http://www.primacom.de/produkte/-primatv/digitaleangebote.php, o.J., Stand: 02.12.2004

o.V., o.J.(7): Digitales Pay-TV, in Internet: http://www.satland.de/Themen/DVB/-Pay-TV/pay-tv.html, o.J., Stand: 19.12.2004

o.V., o.J.(8): Einleitung, in Internet: http://www.digitalfernsehen.de/home/-home_2905.html, o.J., Stand: 19.10.2004

o.V., o.J.(9): Fragen zu ish Plus TV? in Internet: http://www.ish.de/service/-ishdigital/faq.html, o.J., Stand: 01.12.2004

o.V., o.J.(10): Industry Co-operation, in Internet: http://www.irdetoaccess.com/-ias0003.asp, o.J., Stand: 02.11.2004

o.V., o.J.(11): Infos für Einsteiger, in Internet: http://www.premiere.de/content/-abonnieren_premiere_fuer_einsteiger.jsp, o.J., Stand: 13.10.2004

o.V., o.J.(12): ish Plus TV – Preisübersicht, in Internet: http://www.ish.de/ishtv/-digital/plus/preise.html, o.J., Stand: 01.12.2004

o.V., o.J.(13): ish International TV, in Internet: http://www.ish.de/ishtv/digital/-international/index.html, o.J., Stand: 01.12.2004

o.V., o.J.(14): Kabel Digital International, in Internet: http://www.kabeldeutschland.de/kabeldigital/pakete/digitalinternational.php?p=ct&c=1&KABEL_-DEUTSCHLAND_WEB=2510160c41ae4e48684aa, o.J., Stand: 01.12.2004

o.V., o.J.(15): Kabel Digital, Pakete und Preise, in Internet: http://www.-kabeldeutsch-land.de/kabeldigital/pakete/index.php?p=sn&KABEL_DEUTSCHLAND_WEB=2510160c41ae4e486 84aa, o.J., Stand: 01.12.2004

o.V., o.J.(16): Magic/Matrix Modul, in Internet: http://www.digisatshop.ch/de-ch/-dept_17.html, o.J., Stand: 08.12.2004

o.V., o.J.(17): Pay TV / Pay Radio, in Internet: http://www.google.de/-search?q=cache:QWwCNS3fb9oJ:www.handelswissen.de/servlet/PB/menu/1012356/+bekannteste+Pay-TV&hl=de, o.J., Stand: 03.12.2004

o.V., o.J.(18): Pentacrypt 1.09, in Internet: http://www.la-cafetera.com/magic-soft.htm, o.J., Stand: 07.01.2005

o.V., o.J.(19): Piraterie und verschlüsselte Dienste, in Internet: http://www.der--syndikus.de/briefings/it/it_021.htm, o.J., Stand: 15.11.2004

o.V., o.J.(20): Press Backgrounder Piracy, Pay-TV and AEPOC, in Internet: http://www.aepoc.org/press_service/hi_aeback.html, o.J., Stand: 15.01.2005

o.V., o.J.(21): Robust Technology, in Internet: http://www.irdetoaccess.com/-ias0001.asp, o.J., Stand: 02.11.2004

o.V., o.J.(22): SCM Microsystems Inc. Registered Shares DL -,001, in Internet: http://www.is-asp.pbc.maxblue.de/is-asp/mare0041.html?symbol=SCM.FSE-&isin=&wosid=, o.J., Stand: 11.11.2004

o.V., o.J.(23): Set-Top-Box - Das Tor zu ish Digital TV, in Internet: http://www.-ish.de/service/ishdigital/set-top-box.html, o.J., Stand: 01.12.2004

o.V., o.J. (24): Tarife, in Internet: http://www.pep-com.de/homepage/kcr/kcr_-index_1024.htm, o.J., Stand: 08.02.2005

o.V., o.J.(25): The Problem of Piracy Against Conditional Access Systems, in Internet: http://www.aepoc.org/the_problem/the_problem.htm, o.J., Stand: 21.12.2004

o.V., o.J.(26): The Truth, in Internet: http://www.hackhu.com/, o.J., Stand: 21.12.2004

o.V., o.J.(27): Verschlüsseltes digitales Fernsehen, in Internet: http://www.lfm-nrw.de/lfr/faq/digitalesfernsehen/faq6.php3, o.J., Stand: 31.01.2005

o.V., o.J.(28): Verschlüsselungstiefe, in Internet: http://216.239.59.104/-search?q=cache:YuYNkkFs5ggJ:flexnow.uni%EF%B7%93bam-berg.de/-produkt%09/sicherheitsrichtlinien.htm+definition+verschlsslungstiefe&hl=de, o.J., Stand: 06.12.2004

o.V., o.J.(29): Verschlüsselungs-Verfahren im Überblick, in Internet: http://www.ce-markt.de/CE-Markt-Exklusiv/Digital-TV/digital-tv.html, o.J., Stand: 08.12.2004

Pagenstedt, Georg: Strategische Planung für Anbieter von Abonnementfernse-hen, Diss., Universität zu Köln 1995

Peeck, Klaus: Pay-TV-Sender startet Massenklage gegen Produktpiraten, in Internet: http://www.heise.de/newsticker/meldung/17800, 16.05.2001, Stand: 05.03.2005

Pötzsch, Florian, 2001a: Premiere-Hehlerbande aufgeflogen, in Internet: http://-alt.digitv.de/news/arc108.html, 01.12.2001, Stand: 06.12.2004

Pötzsch, Florian, 2001b: Task Force „E-Security" unterstützt Polizei, in Internet: http://alt.digitv.de/news/arc108.html, 01.12.2001, Stand: 06.12.2004

Pötzsch, Florian, 2001c: Pay-TV-Hack: Freiheitsstrafe bis zu zehn Jahren, in Internet: http://alt.digitv.de/news/arc108.html, 02.12.2001, Stand: 06.12.2004

Pötzsch, Florian: „Den Hackern das Handwerk legen!", Interview von Florian Pötzsch mit Humax-Geschäftsführer Franz Simais, in Internet: http://www.-tkv.com/news.php?sprache=deu, 18.10.2002, Stand: 03.12.2004

Pötzsch, Florian: Premiere: Schwarzseher kosten 100 Millionen Euro jährlich, in Internet: http://www.digitalfernsehen.de/news/news_2205.html, 23.10.2003, Stand: 29.10.2004

Porteck, Stefan, 2004a: Premieres Verschlüsselung verärgert Abonnenten, in Internet: http://www.heise.de/newsticker/meldung/46230, 02.04.2004, Stand: 20.09.2004

Porteck, Stefan, 2004b: Erneuter Ärger mit Premieres Verschlüsselung, in Internet: http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/-46513&words=spo, 14.04.2004, Stand: 16.09.2004

Posewang, Wolfgang: Der richtige Schlüssel, in: rfe radio fernsehen elektronik, Nr. 5, 2004, S. 38-39, in Internet: http://www.rfe-online.de/_archiv/frei/-RFE0504-38.pdf, 2004, Stand: 26.12.2004

Rother, Hans-Walther: Pay-TV: Lukrative Aussichten, in: Infosat, 8. Jahrgang, Heft 5, Nr. 74, Mai 1994

Röttgers, Janko: Gut bezahlte Pay-TV-Hacker, in Internet: http://www.heise.de/-tp/r4/artikel/12/12082/1.html, 13.03.2002, Stand: 08.12.2004

Scheffel, Uwe: Attacke gegen Premiere und Co.: Pay-TV ohne Smartcard, in Internet: http://www.de.tomshardware.com/video/20020131/, 31.01.2002, Stand: 25.12.2004

Schembri, Carmen: RE: FW: Frage zur Finanzierung der AEPOC, carmen.-schembri@skynet.be, Absendedatum der E-Mail: 23.01.2005

Schlomski, Jürgen: Digitalfernsehen: Wie und weshalb wird verschlüsselt?, in Internet: http://www.ce-markt.de/CE-Markt-Exklusiv/Digital-TV /digital-tv.-html, Stand: 08.12.2004

Schmerer, Kai: Premiere erwirkt Verfügung gegen Smartcard-Händler, in Internet: http://www.zdnet.de/news/business/0,39023142,2138819,00.htm, 26.08.2003, Stand: 21.09.2004

Schubert, Juliane, 2004a: Feldtester für das neue AlphaCrypt TC gesucht, in Internet: http://www.digitalfernsehen.de/news/news_17331.html, 19.10.2004, Stand: 20.10.2004

Schubert, Juliane, 2004b: Fernsehpiraten schwächen asiatische TV-Industrie, in Internet: http://www.digitalfernsehen.de/news/news_17641.html, 27.10.2004, Stand: 29.10.2004

Schubert, Juliane, 2004c: Premiere-Verschlüsselung bald auch in Polen, in Internet: http://www.digitalfernsehen.de/news/news_19852.html, 17.12.2004, Stand: 20.12.2004

Schumann, Matthias, Hess, Thomas: Grundfragen der Medienwirtschaft, Berlin, Heidelberg 2000

Schwenk, Jörg: Systemsicherheit Teil 4: Pay-TV, in Internet: http://www.nds.-ruhr-uni-bochum.de/lehre/vorlesungen/systemsicherheit /Systemsicherheit-_4.pdf, Stand: 24.02.2005

Sewczyk, Jürgen: Stand der Technik und Tendenzen für die Zukunft neuer Systeme, in: Pay-TV - Technische Grundlagen, Erfahrungen, Wirtschaftlichkeit

und Zukunftsaspekte, hrsg. von: Verband privater Rundfunk und Telekommunikation (VPRT), Bonn 1991

Shepardson, David: Pay-TV providers threaten to sue over service thefts, inInternet: http://www.detnews.com/2002/wayne/0212/13/b03-30073.htm, 08.12.2002, Stand: 05.01.2005

Stiglitz, Joseph E., Schönfelder, Bruno: Finanzwissenschaft, 2. Auflage (1. dt. sprachige Auflage), München 1989

Tetzner, Karl: Die technischen Kenndaten und Bewertung der eingeführten Pay-TV-Systeme, in: Pay-TV - Technische Grundlagen, Erfahrungen, Wirtschaftlichkeit und Zukunftsaspekte, hrsg. von: Verband privater Rundfunk und Telekommunikation (VPRT), Bonn 199

Wadlinger, Christof: Premiere beflügelt die Phantasien, in Internet: http://www.-wuv.de/news/artikel/2005/02/40162/index.html, 22.02.2005, Stand: 25.02.2005

Weidner, Markus: Premiere will mit Werbung aus den roten Zahlen kommen, in Internet: http://www.satundkabel.de/index.php?link=news&newsid=248&ressort=, 23.01.2003, Stand: 25.12.2004

Woll, Artur: Allgemeine Volkswirtschaftslehre, 12. Auflage, München 1996

Xylen: Premiere führt neues Verschlüsselungssystem ein, in Internet: http://-www.winfuture.de/news,10723.html, 01.03.2003, Stand: 16.09.2004

Zimmermann, Phil: Phil Zimmermann über PGP, in: Einführung in die Kryptographie, in Internet: www.rzbd.fh-hamburg.de/ftp/files/kryptografie.pdf, 1999, Stand: 08.12.2004

Zingel, Harry: Was ist das ZKDSG?, in Internet: http://www.bwl-bote.de-/20020322.htm, 22.03.2002, Stand: 25.12.2004

ISSN 0945-8999
ISBN 3-934156-97-5