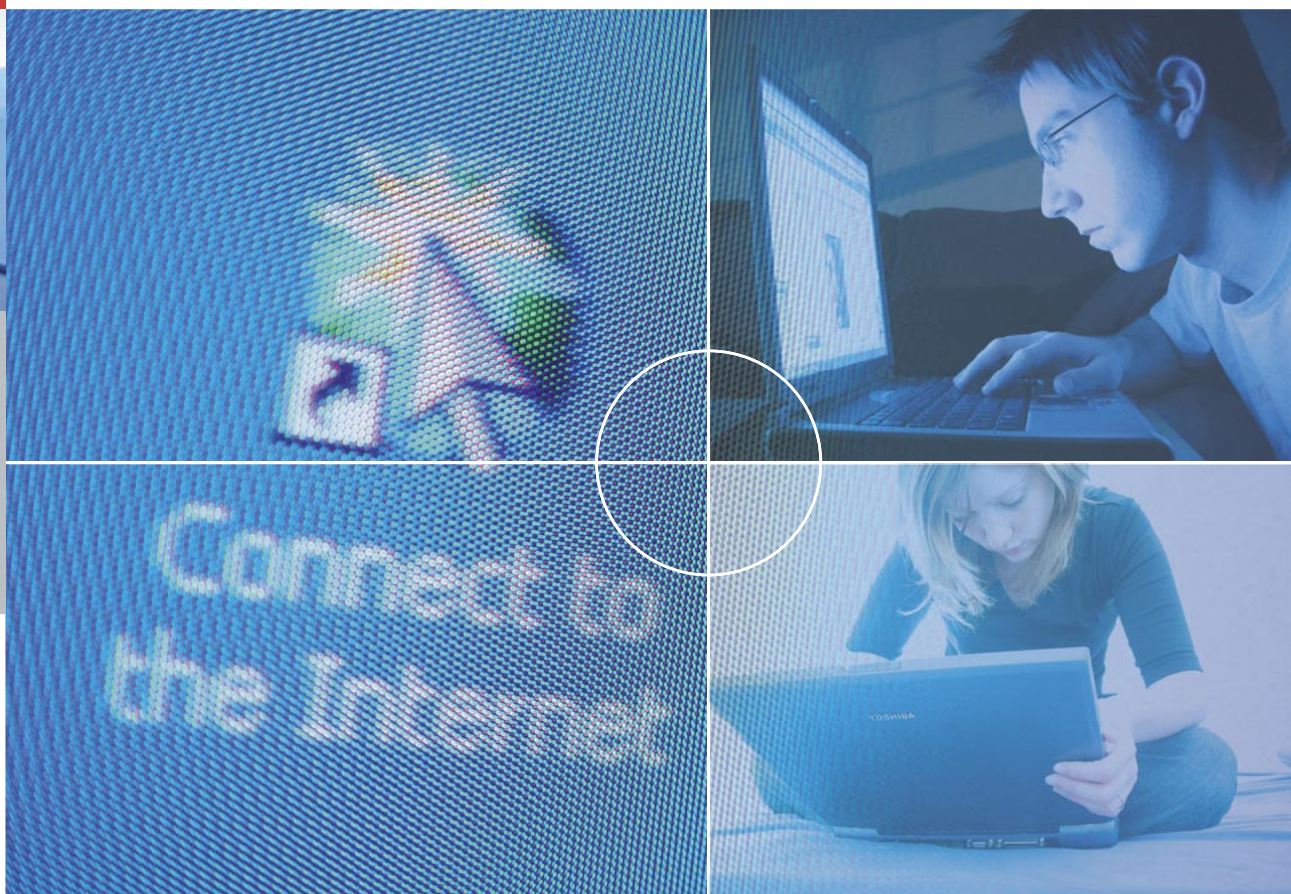
Bundesministerium des Innern

INITIATIVE D21

Effektive Betrugsbekämpfung
Projektbericht



DANKSAGUNG

Großer Dank gilt allen Beteiligten, die in der Projektgruppe Effektive Betrugsbekämpfung mitgewirkt haben. Ihre kritischen Hinweise und konstruktiven Lösungsvorschläge sind in die Erstellung des vorliegenden Berichts eingeflossen.

Ein herzlicher Dank gilt gleichzeitig allen Unternehmen und Organisationen, die durch aktive Mitarbeit in der Initiative D21 das gemeinsame Ziel fördern, Vertrauen und Sicherheit im Internet zu steigern.

Teilnehmer der Projektgruppe sind:

Rolf Bender	Bundesministerium für Wirtschaft und Arbeit
Torsten Bulik	Siemens AG
Anja Bundschuh	eBay International AG (Leitung der Projektgruppe)
Cristin Cordes	Ministerium des Innern des Landes Brandenburg
Michael Denck	Sperr e.V. Verein zur Förderung der Sicherheit in der Informationsgesellschaft
Jens Dohmgoergen	bvh - Bundesverband des Deutschen Versandhandels e.V.
Dirk Eberle	Siemens AG
Joachim Eschemann	Deutsches Forum für Kriminalprävention
Harald Duerkop	KarstadtQuelle AG
Frank Gehde	Landeskriminalamt Berlin
Stefan Grieger	Otto Group
Stefan Grosse	Bundesministerium des Innern (stellvertretende Leitung der Projektgruppe)
Werner Gugetzer	WG IT-Consulting Fernmeldeanlagenelektronik
Christian Hacker	Siemens AG
Otto-Max Herbstritt	Rhoen Klinikum AG
Anke Heuermann	T-Mobile Deutschland GmbH
Hildegard Hils	INET e.V. Internationales Netzwerk Weiterbildung
Stephan Husemann	Bundesministerium der Justiz
Juergen Järnecke	Infineon Technologies AG
Robert Jäger	Bundeskriminalamt
Esther Klein	BAG Bundesarbeitsgemeinschaft der Mittel- und Großbetriebe des Einzelhandels e.V.
Torsten Kobow	Landeskriminalamt Sachsen-Anhalt
Joern Kreitlow	Bundeskriminalamt
Hartwig Kreutz	Bundesamt für Sicherheit in der Informationstechnik
Herbert König	Landeskriminalamt Nordrhein-Westfalen
Tillmann Kübler	Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK)
Karsten Lauber	Bayerisches Landeskriminalamt
Thomas Leitert	TimeKontor AG
Bernhard Lüffe	GAD eG
Gerald Lumma	T-Mobile Deutschland GmbH
Ulrich Martinius	BAG Bundesarbeitsgemeinschaft der Mittel- und Großbetriebe des Einzelhandels e.V.
Garlev Meyer	Landeskriminalamt Schleswig-Holstein
Karl-Heinz Müller	Landeskriminalamt Brandenburg
Wolf-Rüdiger Moritz	Infineon Technologies AG
Manfred Müller	VISA International
Thorsten Neumann	Motorola Global Security
Anja Rodekamp	EURO Kartensysteme GmbH
Olaf Roik	Hauptverband des Deutschen Einzelhandels (HDE) e.V.
Axel Rösner	T-Mobile Deutschland GmbH
Margit Schneider	EURO Kartensysteme GmbH
Jürgen Schlund	FIDUCIA IT AG
Norbert Seitz	Deutsches Forum für Kriminalprävention
Holger Stange	T-Mobile Deutschland GmbH
Christof Störmann	Siemens AG
Wolfgang Vanscheidt	Fujitsu Siemens Computers GmbH
Irmela von Bibra	Bundesagentur für Arbeit
Samuel Voetter	Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK)
Ralf Wicher	Landeskriminalamt Sachsen

Gliederung

1.	**Die D21-Projektgruppe Effektive Betrugsbekämpfung**	**4**
2.	**Ist-Situation – Phänomenologie des Betruges im Online-Handel**	**6**
2.1	Online-Handel in Deutschland	6
2.2	Kriminalität im Online-Handel	7
2.2.1	Dimension der Kriminalität im Online-Handel	7
2.2.2	Formen der Kriminalität im Online-Handel	9
3.	**Strukturen der Betrugsbekämpfung**	**10**
3.1	Verhaltensorientierte Kriminalprävention	10
3.2	Behördliche Strukturen der Strafverfolgung	12
3.3	Technisch orientierte Präventionsprojekte	13
3.4	Europäische und ausländische Projekte zur IuK-Sicherheit und -Kriminalität	15
4.	**Der Umgang mit Online-Betrug in der Praxis von eCommerce-Unternehmen**	**16**
5.	**Handlungsempfehlungen**	**17**

1. Die D21-Projektgruppe Effektive Betrugsbekämpfung

Aktivitäten der D21-Lenkungsgruppe eGovernment/Sicherheit und Vertrauen im Internet

Vertrauen in die Sicherheit des Internets ist eine zentrale Voraussetzung für die soziale und ökonomische Akzeptanz dieses zukunftsträchtigen Mediums und seiner Anwendungen. Seit Gründung der Initiative D21 1999 findet das Thema Vertrauen und Sicherheit in der Informationsgesellschaft hohe Aufmerksamkeit. Der Schutz der IT-Systeme ist nicht nur eine Frage technischer Lösungen, sondern entsteht im Zusammenspiel mit der Aufklärung der Nutzer zum Eigenschutz. Technische Lösungen sind zweifelsohne ein wesentlicher Sicherheitsbaustein. Sie zeigen jedoch erst dann ihre Wirkung, wenn sie (richtig) eingesetzt werden und die Anwender wissen, dass sie und wie sie auf ihre Funktionstüchtigkeit zählen können. Sicherheit kann relativ schnell durch bestimmte Maßnahmen, wie etwa durch die Wahl eines sicheren Passwortes oder die Befolgung bestimmter Verhaltensregeln, verbessert werden. Das Vertrauen der Anwender entsteht dahingegen in einem Prozess, in dem einerseits Internetanwendungen und -abläufe kontinuierlich ihre Verlässlichkeit zeigen und andererseits die Anwender ihr Wissen über mögliche Gefahren und entsprechende Vorbeugemechanismen erweitern.
Die Mitglieder des D21-Lenkungsgruppe eGovernment/ Sicherheit und Vertrauen im Internet sind sich einig, dass wirksame Sicherheit im Internet des Einsatzes und der Anstrengung aller Beteiligten bedarf. Nur wenn Hersteller, Betreiber, Nutzer und Staat sich der Zukunftsaufgabe gemeinsam stellen, kann das Ziel einer sicheren und zukunftsorientierten Informationsgesellschaft erreicht werden.

Derzeit schwächen Diskussionen und Berichte über Betrugshandlungen oder sonstige schädigende Handlungen im Internet das Vertrauen insbesondere der Verbraucher in den elektronischen Geschäftsverkehr.

Um dieser Entwicklung vorzubeugen und die Chancen zu nutzen, die das Internet sowohl gesamtökonomisch als auch für die Gesellschaft der Bundesrepublik bietet, haben verschiedene D21-Projekte im Bereich eGovernment/Sicherheit und Vertrauen im Internet dieses Thema aufgegriffen.
So unterstützt D21 die Internet-Nutzer durch den bereits im Herbst 2001 vorgelegten Leitfaden „IT-Sicherheitskriterien im Vergleich“, der sich insbesondere an Unternehmen des Mittelstands richtet. Der Leitfaden vermittelt IT-Herstellern, -Dienstleistern, und -Anwendern einen Überblick über die gängigen Kriterien für IT-Sicherheit und gibt Handlungsempfehlungen für deren Anwendung.
Weiterhin unterstützt D21 die Einrichtung einer Notrufnummer für die Informationsgesellschaft, die zum 1. Juli 2005 in Deutschland eingeführt wurde. Über sie kann jeder Verbraucher z. B. das Sperren seiner verloren gegangenen Kredit- oder EC-Karte oder sensibler Online-Berechtigungen veranlassen, sofern sich die Herausgeber dem Sperr-Notruf angeschlossen haben.
Aktuell laufende Projektgruppen beschäftigen sich mit Fragen der digitalen Signatur, der Identifizierung und Authentifizierung in der virtuellen Welt sowie der Entwicklung eines Versicherungsschutzes und Risikomanagements für IT/TK-Infrastruktur.

Aufgabenstellung und Arbeit der Projektgruppe Effektive Betrugsbekämpfung

Ziel der Gründung des Projektes Effektive Betrugsbekämpfung im Jahre 2003 war es, das Thema „Betrugsbekämpfung im Internet“ zu untersuchen und nach Wegen zu suchen, die die Betrugsgefahr aus Sicht des Verbrauchers reduzieren und damit letztendlich sein Vertrauen in das Internet steigern. Die Ausgangsfragen waren:

- Was sind die Rahmenbedingungen und Voraussetzungen für eine pro-aktive und re-aktive Betrugsbekämpfung im Netz?
- Was ist unter heutigen rechtlichen Rahmenbedingungen möglich, welche rechtlichen Veränderungen sind für effektive Betrugsbekämpfung erforderlich?
- Was sind die „Best Practices“ der Betrugsbekämpfung?
- Wie können Diensteanbieter (Access Provider, Host Provider, Content Provider) und Ermittlungsbehörden besser zusammenarbeiten?

Im Oktober 2003 fand das Kick-off-Meeting in Berlin statt. Der Teilnehmerkreis dieses Treffens sowie der spätere Mitgliederkreis der Projektgruppe Effektive Betrugsbekämpfung setzt sich aus Vertretern von Unternehmen und Verbänden, die unter anderem im Online-Handel und Online-Banking aktiv sind, sowie Strafverfolgungs- und Regierungsbehörden und Präventionsgremien zusammen.

Die Erwartungen der Mitglieder gingen in zwei Richtungen. Zum einen wurde die Notwendigkeit betont, einen Informationsaustausch zwischen allen relevanten Gruppen zu etablieren und die Sitzungen der Arbeitsgruppe dafür als Ausgangspunkt zu nehmen. Zum anderen wurde die Etablierung eines außenwirksamen Projekts mit der Zielrichtung vertrauensbildender und aufklärender Maßnahmen als sinnvoll erachtet.

Der Arbeitsplan sah vor, eine Bestandsaufnahme der Dimension und Formen von Kriminalität im Umfeld des Online-Handels sowie der gesetzlichen Grundlagen, Möglichkeiten und Strukturen der Strafverfolgung zu erstellen. Um ein Bild der praktischen Erfahrungen der Industrie mit der Bekämpfung von Betrugskriminalität im Internet zu erhalten, sollte eine durch ein unabhängiges Forschungsinstitut durchgeführte anonyme Befragung von Marktplatzbetreibern und eShops veranlasst werden. Die Absicht war, auf Basis dieser Ergebnisse eine Handlungsempfehlung zu verabschieden. In Abgrenzung der bereits innerhalb von D21 bzw. Verbänden laufenden Initiativen zum Thema Sicherheit war man sich einig, den Schwerpunkt der Handlungsempfehlung auf die Aufklärung des Verbrauchers und die Verbesserung des präventiven Schutzes durch die Nutzer selbst zu legen.

Die Umsetzung des Arbeitsplans erfolgte in virtuellen Arbeitsgruppen. Der nun vorliegende Bericht fasst das Ergebnis zusammen und schließt die Arbeit der Projektgruppe ab. Die vorgeschlagenen Handlungsempfehlungen richten sich nicht nur an den Kreis der D21-Mitglieder, sondern an einen weiteren Kreis von Akteuren im Bereich Online-Handel. Die Teilnehmer der Projektgruppe plädieren dafür, dass D21 alle Anstrengungen unternehmen sollte, die in diesem Bericht enthaltenen Handlungsempfehlungen aufzugreifen und deren Umsetzung zu realisieren.

2.1 Online-Handel in Deutschland

Das Internet ist als Träger von Kommunikation und Information sowie als eCommerce-Plattform zu einer treibenden Kraft für wirtschaftliche und soziale Entwicklung und somit zu einer Schlüsseltechnologie geworden. 2005 wird nach einer Studie des Marktforschungsunternehmens eTForecasts die Zahl der Internet-Nutzer weltweit auf über eine Milliarde steigen. Der größte Teil des Zuwachses kommt demnach aus Ländern in Asien, Lateinamerika und Europa.[1]

In der Bundesrepublik Deutschland nutzte im Jahr 2005 mehr als die Hälfte der Bevölkerung ab 14 Jahren (55,1 %) das Internet. Zu diesem Schluss kamen die Initiative D21 und TNS Infratest im aktuellen (N)ONLINER Atlas. Darüber hinaus planen weitere 6 % den Einstieg in die Internetnutzung innerhalb der nächsten 12 Monate. Das Durchschnittsalter der Internetnutzer steigt langsam an und beträgt 39 Jahre (2004: 38,5).[2]

Etwa 60 % der Internetnutzerinnen und -nutzer tätigten Einkäufe über das Internet.[3] Viele davon bieten auch bei Online-Auktionen mit. Untersuchungen im Auftrag der Postbank zum Thema eCommerce kamen für 2004 zu dem Ergebnis, dass die Bezahlung nach Rechnungsstellung mit gut 78 % die immer noch häufigste Zahlungsart ist, gefolgt von Online-Überweisungen und Kreditkartenzahlungen mit jeweils etwa 60 %.[4]

Laut einer Studie des Marktforschungsinstituts European Information Technology Observatory (EITO) waren die Deutschen 2004 im europaweiten Vergleich der Spitzenreiter im Bereich Online-Handel. Mit 202,6 Mrd. Euro entfielen 30 % des Umsatzes im europäischen Onlinehandel auf Deutschland. Bis zum Jahr 2008 wird allein für Deutschland mit einem Zuwachs auf 670 Mrd. Euro gerechnet. Für den Bereich Business-to-Consumer (B2C) prognostiziert der Hauptverband des Deutschen Einzelhandels für 2005 Umsätze im Online-Handel in Höhe von 14,5 Mrd. Euro. Dies entspricht einer Steigerung gegenüber 2004 von etwa 13 %. Der Umsatz 2004 betrug schätzungsweise 13 Mrd. Euro (+17 % zum Vorjahr).

1 eTForecasts Pressemitteilung vom 27.09.2004.

2 (N)ONLINER Atlas 2005, TNS Infratest und Initiative D21, S. 12.

3 Statistisches Bundesamt: Informationstechnologie in Unternehmen und Haushalten 2004, Wiesbaden 2005.

4 Postbank/Europressedienst Research: eCommerce 2004 – Strukturen und Potenziale des eCommerce in Deutschland aus Kunden- und Händlersicht, November 2004. Bei der Befragung waren Mehrfachnennungen möglich.

2.2 Kriminalität im Online-Handel

2.2.1 Dimension der Kriminalität im Online-Handel

Bedeutung von Internetsicherheit für den eCommerce

Sicherheitsbedenken stellen einen der wichtigsten Gründe dar, warum Internet-User das Internet noch zurückhaltend für Online-Einkäufe nutzen.[5] Zu diesem Ergebnis kommt eine Studie der Postbank in Zusammenarbeit mit dem Europressedienst aus dem Jahr 2004, die die Strukturen und Potenziale des eCommerce in Deutschland auslotet. Demnach basiert die Unsicherheit von Neukunden zum einen auf der Unerfahrenheit, zum anderen spielt aber auch die fehlende Aufklärung über die konkreten Sicherheitsvorkehrungen der einzelnen Händler eine Rolle. Dies führt dazu, dass über 70 % der befragten Internetnutzer schon einmal einen Kaufvorgang abgebrochen haben. Im Zuge positiver Erfahrungen nehmen die Bedenken dann zwar ab, doch selbst erfahrene Online-Kunden kaufen nicht völlig angstfrei.[6]
Viele Studien zeigen, dass die Internetnutzer bei ihren eigenen Sicherheitsvorkehrungen oftmals überfordert sind.[7] Zwar ist das Wissen zu Angriffsmöglichkeiten über das Internet hoch, jedoch schützen sich die deutschen Internetnutzer nicht ausreichend.[8] Virenprogrammen, Firewalls und dem regelmäßigen Schließen von Sicherheitslücken durch „patches“ schenken zu viele Internetnutzer noch zu wenig Aufmerksamkeit. Dabei ist zu bedenken, dass unsichere Rechner die gesamte IT-Infrastruktur gefährden, da Angreifer sich vorzugsweise die Sicherheitslücken zu Nutze machen, die bei vielen Anwendern zu finden sind.[9]

Datenlage Internetkriminalität

Die Dimension der Internetkriminalität in Deutschland lässt sich bislang nicht eindeutig beziffern. Festzustellen ist, dass das Problem in der Öffentlichkeit durch einzeln herausgegriffene Fälle oftmals verzerrt und überspitzt dargestellt wird. Zum anderen werden Kriminalitätsstatistiken auf Länderebene veröffentlicht, die zwar zum Teil Betrachtungen für den Online-Handel ausweisen, deren Daten aber (noch) nicht hinreichend genau verglichen werden können, da die zugrunde liegenden Kategorien nicht einheitlich definiert sind. Auch hat die Polizeiliche Kriminalstatistik (PKS) des Bundeskriminalamtes (BKA) bis zum Jahre 2003 das Tatmittel Internet nicht gesondert ausgewiesen. Vor diesem Hintergrund wurde zum 01.01.2004 in der PKS die Sonderkennung „Tatmittel Internet“ eingeführt, um künftig relativ verlässliche Angaben über die Anzahl derartiger Delikte zu erhalten. Die Veröffentlichung der PKS 2004 erfolgte am 9. Juni 2005. Da die Neuerfassung allerdings noch nicht in allen Bundesländern[10] umgesetzt wurde, ergibt sich bislang nur ein erster Überblick, der im Laufe der kommenden Jahre konsolidiert werden wird.

Offizielle Kriminalstatistiken helfen bei der Beurteilung der Tragweite von Online-Kriminalität nicht weiter. Dazu müssten zum einen die Fallzahlen in Bezug zur Zahl aller Online-Aktivitäten gesetzt werden. Eine solche Zahl ist aber nicht ermittelbar. Zudem ist davon auszugehen, dass viele Straftaten im Internet gar nicht zur Anzeige gelangen (Dunkelziffer).[11] Diese Taten fließen dann nicht in die Kriminalstatistiken, wirken sich aber auf das Vertrauen im Internet gleichermaßen aus.

5 Postbank/Europressedienst Research: eCommerce 2004 – Strukturen und Potenziale des eCommerce in Deutschland aus Kunden- und Händlersicht. November 2004. S.17

6 Ebd.: S.33f

7 So auch: D21/AOL Deutschland/TNS Emnid (2005): Sicherheit im Internet. Und Bundesamt für Sicherheit und Informationstechnik (BSI/TNS Emnid (2005): Bürger zu sorglos im Internet.

8 So der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) Dr. Udo Helmbrecht zur Veröffentlichung der BSI-Studie zur IT-Awareness in Deutschland am 20. Januar 2005. Siehe auch unter: www.bsi.bund.de/presse.

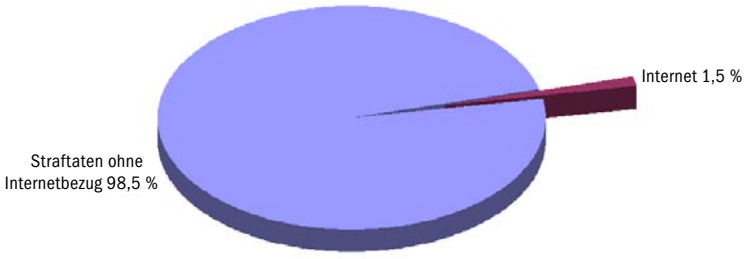
9 Ebda.

10 Erfasst wurden Straftaten aus zehn Bundesländern: Schleswig-Holstein, Bremen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und Thüringen

11 Bundeskriminalamt, Bundeslagebild IuK-Kriminalität 2003, S. 10.

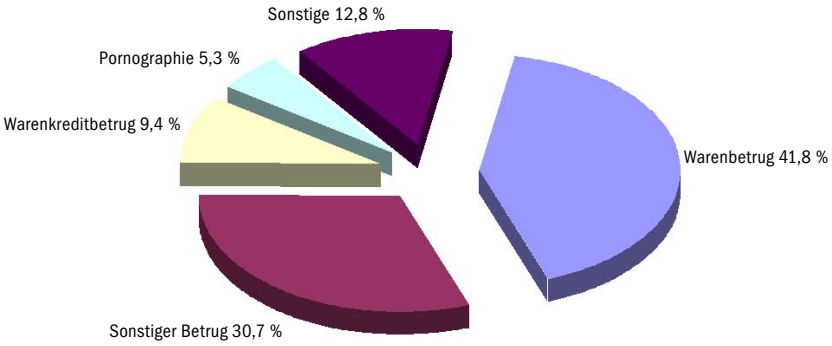
Im Folgenden soll daher ein Eindruck von den Dimensionen gegeben werden, wie er sich nach Einschätzung der Projektgruppe darstellt. Festzuhalten ist, dass es sich hierbei um eine Zustandsbeschreibung, nicht jedoch um eine Entwicklung handelt. Hierzu wird auf die Zahlen der PKS 2004[12] für Straftaten unter Benutzung des Tatmittels Internet zurückgegriffen, denen das Phänomen Betrug im Online-Handel zuzurechnen ist. Unter Betrugsdelikte mit Tatmittel Internet werden dort Waren- und Warenkreditbetrug, sonstiger Betrug, Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten, weitere Betrugsarten sowie Computerbetrug gezählt. Von den insgesamt für Deutschland erfassten Straftaten wurden 1,5 % mittels des Tatmittels Internet begangen. Der überwiegende Teil hiervon wurde im Bereich Betrug verzeichnet (81,9 %), gefolgt von der Verbreitung pornographischer Schriften (5,3 %), von Straftaten im Zusammenhang mit Urheberrechtsbestimmungen (3,9 %) und der Datenveränderung/Computersabotage (2,7 %). Als Tendenz verzeichnet die PKS 2004, dass die Steigerung beim Waren- und Warenkreditbetrug von 19,3 % gegenüber dem Vorjahr insgesamt wohl zu einem erheblichen Teil auf die zunehmende Nutzung und Bedeutung des Internets und von Internetauktionen zurückgeführt werden kann.[13]

Abbildung 1: Straftaten mit Tatmittel Internet 2004



Quelle: PKS 2004

Abbildung 2: Zusammensetzung Straftaten mit Tatmittel Internet 2004



Quelle: PKS 2004

Es ist festzustellen, dass das Internet in den letzten Jahren zunehmend von Tätern in den verschiedensten Deliktbereichen zur Begehung von Straftaten genutzt worden ist. Mit einer weiteren Steigerung der Fallzahlen ist, angesichts der allgemein steigenden Bedeutung des Mediums, nahezu zwangsläufig zu rechnen.
Zumeist sind es „tradierte“ und im Strafrecht längst geregelte Kriminalitätsformen wie z. B. Betrug, für die die technologischen Möglichkeiten des Internets lediglich eine neue Tatgelegenheit bieten. Besonders die vermeintliche Anonymität dürfte das Medium für viele Täter im ersten Moment besonders attraktiv erscheinen lassen. Die steigenden Aufklärungsquoten in den letzten Jahren zeigen jedoch, dass sich die Anzeige von Straftaten im Internet lohnt. Kommt es zur Anzeige und damit zu polizeilichen Ermittlungen, verzeichnet die PKS 2004 eine sehr hohe Aufklärungsquote von beispiels-

12 Polizeiliche Kriminalstatistik 2004. Siehe unter: http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Broschueren/2005/Polizeiliche__Kriminalstatistik__2004__de.html

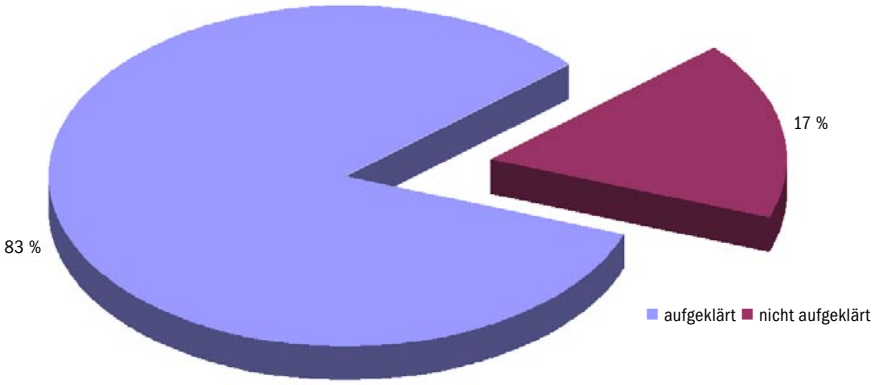
13 Polizeiliche Kriminalstatistik, S. 5.

weise 94 % beim Waren- und Warenkreditbetrug. Sowohl Strafverfolgungsbehörden als auch Industrie können zunehmend Erfolge bei der Bekämpfung von Internetbetrug verzeichnen. Das ist letztendlich eine positive Perspektive. Die Erfahrungen von Behörden und Betroffenen mit dem Tatmittel Internet zeigen, dass der richtige Einsatz von Prävention, Aufklärung und Strafverfolgung wirkt. Derzeit ergeben sich mit neuen Phänomenen wie dem sog. Phishing[14] neue Herausforderungen für Industrie und Strafverfolgungsbehörden, weil hier zunehmend gegen international organisierte Tätergruppierungen vorgegangen werden muss.

2.2.2 Formen der Kriminalität im Online-Handel

Kaufverträge und andere Rechtsgeschäfte unterliegen online wie offline im Wesentlichen den gleichen Bedingungen. Ein Verkäufer möchte etwas verkaufen, der Käufer etwas erwerben. Sind sich beide einig, kommt ein Kaufvertrag zustande, der abgewickelt werden muss (Zahlung, Übergabe des Kaufgegenstandes). Einerseits wird der Verbraucher bei Online-Geschäften durch ein besonderes Widerrufs- und Rückgaberecht geschützt (§§ 312b ff BGB), andererseits bietet die Tatsache, dass der Online-Handel im Fernsabsatz erfolgt und sich die Parteien nicht persönlich gegenüberstehen und dadurch nicht leicht einschätzen können, Möglichkeiten für kriminelle Aktivitäten. In der Mehrzahl der Fälle zählen Internetbetrüger auf die Unwissenheit bzw. Unerfahrenheit ihrer Opfer im Umgang mit dem Internet.

Abbildung 3: Aufklärungsquote bei Straftaten mit Tatmittel Internet 2004



Quelle: PKS 2004

In vielen Fällen handelt es sich bei Internet-Straftaten um klassische Delikte, die trotz der neuartigen Begehungsformen mit den vorhandenen Strafvorschriften erfasst werden können. Ein Beispiel hierfür ist der Betrug (§ 263 StGB), der mit seinen abstrakten Tatbestandsmerkmalen auch Tatbegehungen über das Internet erfassen kann. Ergänzt wird diese Tat durch den Computerbetrug (§ 263a StGB), der auch Fälle erfasst, wenn nicht Menschen getäuscht, sondern technische Einrichtungen überlistet werden. Viele andere Delikte etwa zum Schutz der Privatsphäre oder der Sicherheit im Rechtsverkehr können zudem einschlägig sein. So wird in der Regel die Registrierung bei einem Diensteanbieter unter falschem Namen, also der sog. Identitätsmissbrauch, von bestehenden Straftatbeständen, wie in diesem Fall § 269 (Fälschen beweiserheblicher Daten) erfasst. Probleme können sich allerdings immer wieder bei Auslegungsfragen und insbesondere bei der Tatermittlung ergeben.

Neben diesen Betrugsformen, die in erster Linie zum wirtschaftlichen Schaden beim Verbraucher führen, sind weitere Straftaten zu nennen. Die Verletzung von Urheber- und Markenrechten von Dritten ist ein Beispiel.

Ungeachtet der Frage, welcher Straftatbestand vorliegt, war für die Arbeit der Projektgruppe entscheidend, mit welchen Ansätzen kriminelle Aktivitäten eingedämmt bzw. unterbunden werden können.

14 Phishing: Form von Internetmissbrauch, bei welchem versucht wird, vertrauliche Informationen des Internnutzer wie z. B. Kontonummer, PIN-Code, Kreditkartennummern oder Online-Passwörter durch verschiedene Methoden zu erlangen Häufig erhält dabei der Internnutzer eMails, die genauso aussehen wie die eines bekannten Unternehmens mit zumeist hohem Markenbekanntheitsgrad wie Banken, Kreditkartenfirmen oder eCommerce-Unternehmen. In der eMail wird behauptet, das Konto, die Kreditkarte oder der Online-Account sei kompromitiert worden und man habe persönliche Informationen wie Kontonummer, PIN-Code, Kreditkartennummern oder Online-Passwörter in ein Webform einzugeben, auf das man über einen in der Mail angebenen URL-Link gelangt. In dem Moment der Herausgabe der Informationen können die Betrüger damit weitere kriminelle Aktivitäten begehen.

3.1 Verhaltensorientierte Kriminalprävention

Eine der wichtigsten Rollen bei der Betrugsbekämpfung spielt die Aufklärung der Internetnutzer als mögliche Opfer. Denn der beste Schutz des Einzelnen ist die Kenntnis des Gefahrenpotenzials und das entsprechende Abstimmen der persönlichen Verhaltensweisen. Dazu gehört es, Fehler und Nachlässigkeiten zu vermeiden sowie aktuelle Sicherheitsfunktionen und -technologien richtig zu nutzen. Mit diesem Wissen als Basis kann der Internetnutzer letztlich die Gefahren besser einschätzen und selbst entscheiden, welchen Angeboten und Möglichkeiten des Internets er Vertrauen schenken kann. Alleine in Deutschland existiert eine Vielzahl von Initiativen und Angeboten an verschiedene Zielgruppen, wie Eltern und Lehrer, Privatnutzer oder mittelständische Unternehmen. Im Folgenden sollen einige Beispiele aufgezeigt werden, die den Internetnutzern Hilfestellungen zum sicheren, selbstverantwortlichen Umgang mit dem Internet geben.

Polizeiliche Kriminalprävention (ProPK)

Das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) – bis 1997 KPVP genannt – verfolgt seit 1965 das Ziel, die Bevölkerung, Multiplikatoren, Medien und andere Präventionsträger über Erscheinungsformen von Kriminalität sowie über Möglichkeiten zu deren Verhinderung aufzuklären. Dies geschieht hauptsächlich über Massenmedien und bundesweite Aktionen. Mit zahlreichen Broschüren, Faltblättern sowie weiteren Print- und Online-Medien stehen der Polizei und den Multiplikatoren der Polizeilichen Kriminalprävention eine Vielzahl von hochwertigen Hilfsmitteln zur Verfügung, mit denen eine gezielte Präventionsarbeit gegenüber den Bürgern möglich wird. Die Polizeiliche Kriminalprävention nimmt damit, gerade unter dem Eindruck einer sich rasch weiterentwickelnden Informationsgesellschaft, eine entscheidende Funktion ein.

ProPK Online - Das Vorbeugungsprogramm der Polizei im Internet.
Internet-Adresse: http://www.polizei-beratung.de

Kernstück des weit mehr als 400 Seiten umfassenden Angebots ist die umfangreiche Rubrik Vorbeugung, in der die Kriminalitätsfelder Drogen, Sexualdelikte, Diebstahl/Einbruch, Gewalt, Raub, Betrug, Jugendkriminalität und Gefahren im Internet mit konkreten Tipps behandelt werden.

Informationen zu den „Gefahren des Internets“
Um auf spezifische Gefahren, die im Zusammenhang mit der Nutzung des Internets und seinen vielfältigen Diensten auftreten, reagieren zu können, wurde im Internet-Auftritt der Polizeilichen Kriminalprävention eine dafür eigene Rubrik eingerichtet.
Im Jahr 2004 wurde das Problem der so genannten Phishing-Mails aufgenommen und umfassend beleuchtet.
Kurz vor der Veröffentlichung stehen Informationen zum Thema eCommerce, die in Abstimmung mit Verbänden der Internetwirtschaft und Unternehmen erstellt wurden. Hierbei wird insbesondere das sicherheitsbewusste Nutzen von Online-Angeboten und Online-Auktionen dargestellt. Umfangreiche Tipps und Verhaltenshinweise sollen die Nutzer davor schützen, durch unseriöse Angebote geschädigt zu werden.
Anfang des Jahres 2002 verunsicherten die so genannten 0190-Dialer die „Internet-Gemeinde“. Die missbräuchliche Verwendung von diesen Einwahlprogrammen entwickelte sich zu einer wahren Kostenfalle und verursachte erhebliche finanzielle Schäden. Diese Problematik wurde zeitnah aufgegriffen und erforderliche Sicherheitstipps umfangreich beleuchtet.

„Ins Internet – mit Sicherheit!“ – Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik stellt in seinem Online-Portal www.bsi-fuer-buerger.de grundlegende und einfach verständliche Informationen, Regeln und Vorsichtsmaßnahmen für das Internet zur Verfügung. Das Internet ist neben seinem außerordentli-

chen Nutzen auch eine Quelle für mögliche Angriffe auf Computer und Daten. Zum Schutz gegen solche Angriffe stehen vielfältige Möglichkeiten zur Verfügung. Unabdingbar sind umfassende Information über Gefährdungen und die Umsetzung von entsprechenden Sicherheitsmaßnahmen. Grundlegende Begrifflichkeiten wie zum Beispiel Würmer, Viren, Dialer, Spam und Ähnliches werden erklärt und die entsprechenden Schutzmaßnahmen werden dargestellt.

Leitfaden Handel im Internet – LKA NRW

Das Landeskriminalamt in Nordrhein-Westfalen bedient als Servicedienststelle u. a. durch fachspezifische Materialien für den Deliktsbereich Internetkriminalität die in NRW angeschlossenen 50 Kommissariate, deren Mitarbeiter Kriminalprävention „vor Ort“ - teilweise auch mit örtlichen Beratungsstellen - betreiben. Dazu werden auch für Internetnutzer einfache Leitfäden zum Handel im Internet bereitgestellt.

Präventionsprojekt „Gefahren im Internet“ der Kriminalpolizeiinspektion Kempten (Allgäu)

Die Kriminalpolizeiinspektion Kempten führt seit März 2003 öffentliche Informationsveranstaltungen zum Thema „Gefahren im Internet“ durch. Ergänzend erfolgt eine interne Information der Beamten zur Computer- und IuK-Kriminalität. Das Projekt widmet sich den Themenschwerpunkten „Grundlagen des Internets, Verbreitung pornografischer Schriften, eMail, Computerviren, Kinder im Internet: Kindersicheres Netz, Piraterie und Raubkopie, Tipps für sicheres Surfen, Dialer und Online-Auktionen.“

Kursangebot „Gefahren am PC“ der Polizeidirektion Hannover

Seit April 2002 bietet die Polizeidirektion Hannover regelmäßig Abendkurse zum Thema „Gefahren am PC“ an. Ziel des Kurses ist es, Eltern einen ersten Überblick über das komplexe Thema „Multimedia“ zu geben und die Möglichkeiten der Kontrolle und Gefahren aufzuzeigen. Die Vermittlung von Medienkompetenz der Eltern steht im Vordergrund. Das Thema „Betrug“ wird insbesondere zu den Bereichen 0190/0900-Nummern, Homebanking und Internetauktionen behandelt.

Public-Private Partnership: Initiative „Deutschland sicher im Netz“

Unter der Schirmherrschaft des Bundesministeriums für Wirtschaft und Arbeit haben sich namhafte Unternehmen und Behörden zur Initiative „Deutschland sicher im Netz“ zusammengeschlossen. Neben unterschiedlichen Selbstverpflichtungen, das Internet sicherer zu machen, bietet die Initiative mit ihrem Internetauftritt www.sicher-im-netz.de Hintergrundinformationen und Checklisten für die unterschiedlichen Internetnutzer, von Privatpersonen über Eltern und Lehrer bis hin zu Unternehmen, Behörden und Institutionen.

Sicherheit im Internet für den Mittelstand

Das Bundesministerium für Wirtschaft und Arbeit hat gemeinsam mit dem Bundesministerium des Innern eine Initiative gestartet, die verständliche und mittelstandsspezifische Informationen in einem Online-Portal www.sicherheit-im-internet.de zur Verfügung stellt. Für den Auf- und Ausbau internetbezogener Geschäftsfelder mittelständischer Unternehmen werden fundierte Hinweise für mehr Sicherheit im Internet zur Verfügung gestellt. Diese orientieren sich an einer schnellen und einfachen Umsetzung in den Unternehmen.

3.2 Behördliche Strukturen der Strafverfolgung

Strafverfolgung ist grundsätzlich Sache der Länder. Bisher gibt es im Bereich der Bekämpfung der Internetkriminalität keine einheitlichen Strukturen in den Strafverfolgungsbehörden. In den meisten Bundesländern ist die Bearbeitung der verschiedenen Delikte in die zuständigen Fachdienststellen eingebunden. Internetbetrug wird also von den Dienststellen aufgenommen, in denen auch der „alltägliche" Betrug bearbeitet wird. Die Fachstellen fordern lediglich technische Unterstützung von Datenverarbeitungs-Gruppen an.

Nicht in allen Bundesländern gibt es auf Internetkriminalität spezialisierte Servicedienststellen. In Nordrhein-Westfalen beispielsweise sind landesweit insgesamt ca. 110 Mitarbeiter beim Landeskriminalamt (LKA NRW) und in den Kreispolizeibehörden (KPB) an 50 Standorten sowohl für die DV-Beweissicherung als auch für die Unterstützung bei Delikten mit Internetbezug zuständig. Diese Aufgaben werden in den KPB durch die IT-Ermittlungsunterstützung wahrgenommen, die wiederum von den Dezentralen Informations- und Servicezentren (DISC) bei 6 Großbehörden und dem Zentralen Informations- und Servicezentrum Computerkriminalität (ZISC) beim LKA NRW unterstützt werden. Auch in Sachsen-Anhalt gibt es z. B. neben einer Koordinierungsstelle im Landeskriminalamt (LKA) spezialisierte Servicegruppen, die sowohl im LKA als auch in den Polizeidirektionen angesiedelt sind. Diese Servicegruppen stehen sowohl für die DV-Beweissicherung und –auswertung als auch für die Unterstützung bei Delikten mit Internetbezug zur Verfügung.

Das Landeskriminalamt Berlin hat hingegen eine zentrale Servicestelle für Internetkriminalität (Kriminalkommissariat Internet) eingerichtet. Die Delikte werden auch hier erst einmal bei den zuständigen Fachdienststellen bearbeitet, doch unterstützt das Kriminalkommissariat Internet mit seinen forensischen Kenntnissen die jeweiligen Dienststellen bei der oft schwierigen Ermittlungsarbeit. Die nichttechnischen Ermittlungen verbleiben nach wie vor bei den zuständigen Fachdienststellen.

Auf Bundesebene beschäftigt sich das Bundeskriminalamt mit mehreren Organisationseinheiten mit dem Phänomen der Internetkriminalität. Neben dem Bereich Phänomenologie (Bearbeitung der verschiedensten Delikte, wie Kreditkartenkriminalität im Internet, Kinderpornografie, Dialer, Viren und Würmer) und dem Ermittlungsbereich für IuK[15]-Kriminalität wurde das TeSIT (Technisches Servicezentrum für Informations- und Kommunikationstechnologien) eingerichtet. Schwerpunkt seiner Arbeit ist die technische Unterstützung bei Exekutivmaßnahmen, die Forensik der IuK-Kriminalität und Ermittlungen in Datennetzen, wofür Anfang 1999 die Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD) eingerichtet wurde. Diese übernimmt die Aufgabe einer „Streife im Netz". Straftäter im Internet sollen durch sie identifiziert und überführt werden, um letztlich vor der Nutzung des Internets für kriminelle Zwecke abzuschrecken und strafbare Handlungen zu verhindern (generalpräventiver Aspekt).

Für den länderübergreifenden Wissens- und Informationsaustausch führt das Bundeskriminalamt seit Jahren jährlich Arbeitstagungen für IuK- bzw. Internetsachbearbeiter und für Mitarbeiter der deliktübergreifenden Datenverarbeitungsgruppen durch. 2004 wurde erstmals auch ein Workshop für Internet-Ermittler abgehalten. Des Weiteren koordiniert das Bundeskriminalamt im Rahmen seiner Zentralstellenfunktion länderübergreifende und internationale Ermittlungen.

15 IuK: Informations- und Kommunikationstechnologie

3.3 Technisch orientierte Präventionsprojekte

Datenverarbeitungssysteme weisen spezifische Schwachstellen auf, die von Straftätern genutzt werden können. Durch geeignete technische Maßnahmen lassen sich diese Systeme derart sichern, dass der zu betreibende Aufwand manchmal den Nutzen eines Angriffs nicht mehr rechtfertigen würde. An diesem Punkt bietet die so genannte „technisch orientierte Prävention“ eine weitere Möglichkeit, Betrug im Online-Handel effektiv zu bekämpfen.

Bundesamt für Sicherheit in der Informationstechnik

Das Referat CERT-Bund (Computer Emergency Response Team für Bundesbehörden) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist die zentrale Anlaufstelle für präventive und reaktive Maßnahmen in Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in Computersystemen. Es erstellt und veröffentlicht bspw. Handlungsempfehlungen bei Hard- oder Softwareproblemen. Die Dienstleistungen von CERT-Bund stehen in erster Linie den Bundesbehörden zur Verfügung, je nach Ressourcenlage werden auch private Anfragen bearbeitet. Warn- und Informationsdienste (WID) mit Sicherheitshinweisen und
-warnungen werden allgemein zur Verfügung gestellt. Zudem stellt das BSI im Rahmen seines Internet-Angebotes www.bsi.bund.de eine Vielzahl von Informationen über Möglichkeiten technischer Prävention bereit, z. B. Studien zu Penetrationstests, Firewalls, Intrusion-Detection-Verfahren, praktische Hinweise zum Umgang mit aktiven Web-Inhalten, Programmen mit Schadfunktionen sowie Sicherheit von Web-Servern.

Mcert

Mcert ist eine Initiative unter der Federführung des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) in Form einer Public-Private-Partnership zwischen dem Bundesministerium des Innern und dem Bundesministerium für Wirtschaft und Arbeit sowie kompetenten Industriepartnern. Mcert ist ein neutrales und herstellerunabhängiges Kompetenzzentrum für IT-Sicherheit. Die Leistungen sind speziell auf die Bedürfnisse kleiner und mittlerer Unternehmen abgestimmt.
Mcert bietet Sicherheitsinformationen und Handlungsempfehlungen. Dazu gehören etwa Warnmeldungen zu Schadensprogrammen und Hinweise auf Sicherheitslücken im Sinne eines vorbeugenden Schutzes gegen Bedrohungen der IT-Systeme. Träger von Mcert ist die Mcert Deutsche Gesellschaft für IT-Sicherheit mbH, die eine 100 %-ige Tochter des BITKOM ist.

Notrufnummer 116 116 für die Informationsgesellschaft

Deutschland hat als erstes Land zum 1. Juli 2005 die neue einheitliche Notrufnummer 116 116 zum Sperren von zum Beispiel Kredit- und EC-Karten, Handys, digitalen Signaturen, Krankenkassenkarten, Mitarbeiter-Ausweisen, Kundenkarten oder sensiblen Online-Berechtigungen des Internets eingeführt. Ziel der neuen Notrufnummer ist es, dem Bürger im Notfall eine einfache und unkomplizierte Lösung zur Sperrung seiner Karten und Berechtigungen anzubieten. Dadurch soll auch das Vertrauen der Bürger in neue Technologien gesteigert werden.

Sicheres Bezahlen im Internet

Sowohl für Händler als auch für Käufer ist in Bezug auf Waren- bzw. Warenkreditbetrug eine zuverlässige Abwicklung des Zahlungsvorganges von entscheidender Bedeutung. Wechselseitige Absicherung durch technische Maßnahmen schafft dabei besonders für Neueinsteiger die Grundlage für künftiges Vertrauen.
Im Folgenden werden vier Bezahlsysteme, die den besonderen Anforderungen des Online-Handels gerecht werden, vorgestellt:

Kartenzahlung
Kreditkartenzahlung ist heute schon ein vielfach genutztes Instrument für die Zahlung bei Online-Geschäften. Diese Zahlungsmethode sollte folgenden

zwei Anforderungen genügen. Zum einen wünscht sich der Karteninhaber einen hohen Sicherheitsstandard, zum anderen erwartet der Händler eine Zahlungsgarantie. Mit dem 3D-Secure-Verfahren der Kreditkartengesellschaften schützen sich der Online-Händler und Kreditkarteninhaber vor dem missbräuchlichen Einsatz einer Kreditkarte. Die Anwendung von 3D-Secure stellt sicher, dass es sich bei dem Käufer tatsächlich um den Kreditkarteninhaber handelt. Der Karteninhaber registriert sich bei seiner Bank für 3D-Secure. Hierbei legt er ein Passwort und einen Sicherheitshinweis fest. Beim Einkauf im Internet wählt der Kunde die gewünschten Produkte oder Dienstleistungen aus, legt sie in den Warenkorb und gibt nach Auswahl der Zahlungsart die Daten seiner Kreditkarte ein. Daraufhin erscheint eine Pop-up-Seite seiner Hausbank, auf der der Kunde sein persönliches Passwort eingibt. Die Passworteingabe erfolgt also auf der Seite der kartenausgebenden Bank - dies wird dem Kunden garantiert, indem der von ihm vergebene Sicherheitshinweis auf der Seite zur Passworteingabe angezeigt wird. Die Bank verifiziert das Passwort und gibt dann die Transaktion frei. Sowohl Händler als auch Karteninhaber haben nun die Gewissheit, dass die gegenseitige Identität verifiziert wurde. Das Passwort ersetzt damit sozusagen die Unterschrift bei einem Einkauf an der Ladentheke. Wenn für eine Kreditkarte noch kein Passwort vergeben wurde, funktioniert der Einkauf wie bisher auch ohne Passwort. Trotzdem profitieren die Online-Händler künftig von der Haftungsumkehr (Liability-Shift) seitens Visa und MasterCard: Künftig entfallen für sie die Kosten für zurückgewiesene Abbuchungen, Warenverlust bei Kartenmissbrauch oder für die Abwicklung von Rückzahlungen.

GeldKarte

Die GeldKarten-Funktion kann auf einer ec- oder Kundenkarte der Bank oder Sparkasse durch einen Chip zur Verfügung gestellt werden. Aktuell sind in Deutschland ca. 60 Millionen Karten im Umlauf. Im Prinzip funktioniert das bargeldlose Bezahlen mit der GeldKarte im Internet genauso wie am Parkautomaten oder im Geschäft an der Kasse. Allerdings muss für den Einsatz beim Online-Shopping der Nutzer an seinem Computer ein geeignetes Chipkartenlesegerät (ein sog. Internet-Kundenterminal oder auch „Klasse-3-Leser“) angeschlossen haben. Zur Zahlung schiebt dann der Kunde eine ausreichend geladene (max. 200 Euro) GeldKarte in das Internet-Kartenterminal. Nach der Freigabe der Zahlung durch den Kunden wird der Betrag anonym und sicher über eine SSL-gesicherte Verbindung von dem Chip abgebucht und dem Händler gut geschrieben.

Online-Überweisung

Die Online-Überweisung ist gerade in Deutschland schon heute ein besonders beliebtes Instrument zur Zahlung von Internet-Einkäufen. Dieses Verfahren ist für den Kunden dann einfach und sicher, indem beim Bezahlen per Online-Überweisung der Kunde direkt über eine sichere Verbindung vom Händler an seine Bank weitergeleitet wird, die ihm einen passend vorausgefüllten Überweisungsträger anbietet. Die Legitimation des Kunden erfolgt, wie zuvor mit seiner Bank vereinbart, z. B. über HBCI, PIN/TAN oder eine Signaturkarte. Der Händler erhält als Beleg von der Bank eine sofortige Einreichungsbestätigung und kann daraufhin die logistischen Prozesse für die Lieferung anstoßen.

Online-Bezahlsysteme – „eGeld“

Elektronisches Geld (eGeld) kann als elektronischer Ersatz für Bargeld betrachtet werden, das elektronisch, beispielsweise auf einer Chipkarte oder in einem Computer, gespeichert wird und dazu dient, Zahlungen elektronisch durchzuführen. Mit Blick auf die Sicherheit bieten Online-Bezahlsysteme den wesentlichen Vorteil, dass der Empfänger der Zahlung keinerlei persönliche Informationen des Zahlenden erfahren muss, da diese beim eGeld-Institut, das wie eine Art „Treuhänder“ fungiert, hinterlegt ist. Voraussetzung für die Teilnahme am Verfahren ist in der Regel eine eMail-Adresse, ein Bankkonto sowie die Eröffnung eines Kontos bei einem Anbieter eines Online-Bezahlsystems. Nach Auslösung einer Zahlung wird der Betrag sofort dem Konto des Empfängers gutgeschrieben und eine Benachrichtigung des Empfängers ausgelöst. Dieser kann das so erhaltene Geld auf sein Bankkonto transferieren.

3.4 Europäische und ausländische Projekte zur IuK-Sicherheit und -Kriminalität

Weltweit bietet das Internet über einer Milliarde Menschen die Möglichkeit zum Austausch von Kommunikation und Waren. Es birgt für seine Nutzer aber auch gleiche Risiken und Gefahren. Daher dürfen Projekte und Kooperationen zur effektiven Bekämpfung von Betrug im Online-Handel nicht an den nationalen Grenzen stehen bleiben, sondern müssen sich mit europäischen und internationalen Projekten austauschen. Im Folgenden werden einige Beispiele vorgestellt.

Europäische Agentur für Netz- und Informationssicherheit (ENISA)

Die Europäische Agentur für Netz- und Informationssicherheit wurde Anfang 2004 gegründet und ist erst langsam dabei, ihre Arbeit aufzunehmen. Die Hauptaufgabe von ENISA ist die Förderung einer verstärkten Zusammenarbeit und eines verbesserten Informationsaustausches zwischen den Mitgliedsstaaten zu Themen der Netz- und Informationssicherheit. Dies umfasst auch die Analyse von Informationen über derzeitige und aufkommende Risiken und Probleme sowie die Sensibilisierung von Bürgern, Unternehmen und Verwaltungen für Risiken, die mit der Nutzung des Internets und von Informationssystemen verbunden sind. Die Agentur verfolgt in Kooperation mit der Industrie die Entwicklung der Forschung und Normung.

AGIS-Programm der Europäischen Kommission

Mit dem AGIS-Programm werden in den EU-Mitgliedstaaten und den Kandidatenländern Angehörige der Rechtsberufe, Strafverfolgungsbehörden und Vertreter von Stellen, die mit der Unterstützung der Opfer befasst sind, beim Aufbau europaweiter Netzwerke und dem Austausch von Informationen und bewährten Praktiken unterstützt. Anträge auf die finanzielle Unterstützung von Projekten durch das AGIS können jährlich gestellt werden. Das AGIS-Programm stellte 2005 bspw. Gelder für eine Konferenz zur Sicherheit bei Online-Auktionen zur Verfügung, an der Polizeibeamte aus zehn europäischen Ländern sowie Vertreter der Wirtschaft, des Bundeskriminalamts und verschiedener Landeskriminalämter teilnahmen.

Interpol European Working Party on IT Crime (EWPITC)

Im Rahmen von Interpol bildet die Arbeitsgruppe mit Mitgliedern aus 14 EU-Staaten eine Plattform für den Erfahrungsaustausch zur Bekämpfung von IT-Kriminalität. Ergebnis dieser Kooperation ist u. a. ein Handbuch zur Computer-Kriminalität – „Information Technology Crime Investigation Manual“ – das ständig aktualisiert wird. Der grenzüberschreitende Informations- und Erfahrungsaustausch, die Einrichtung von sog. National Central Reference Points for Computer related Crime sowie die Lösung praktischer (Ermittlungs-) Probleme bilden die Schwerpunkte der Arbeit. Darüber hinaus widmet sich die EWPITC auch der Fortbildung und unterstützt die Länder bei der Planung und Durchführung von Lehrgängen im Bereich IuK-Kriminalität.

Anti-Phishing Working Group

Die US-amerikanische Anti-Phishing Working Group (APWG) ist eine Kooperation zahlreicher Industrie-Unternehmen, die sich mit der Bekämpfung von Identitäten-Diebstahl und Betrug durch Phishing beschäftigt. Sie bildet ein Forum, in dem die Problematik diskutiert und analysiert wird, um durch Informationsaustausch Gegenmaßnahmen zu entwickeln. Dazu gehören auch die Schulung von Personal und die Entwicklung geeigneter Techniken. Die APWG arbeitet mit staatlichen Behörden im Bereich der Strafverfolgung und der Gesetzgebung zusammen.

4. Der Umgang mit Online-Betrug in der Praxis von eCommerce-Unternehmen

Um ein genaueres Bild von der Praxis des Online-Betruges zu bekommen und entsprechende Gegenmaßnahmen zu entwickeln, wurde im Herbst 2004 in Zusammenarbeit mit TNS Emnid von der Projektgruppe „Effektive Betrugsbekämpfung“ eine qualitative Studie zum Thema „Sicherheit im eCommerce“ durchgeführt. In stichprobenartigen, leitfadengestützten Telefoninterviews (Teilnehmer: Sechs Online-Versandhandelsunternehmen und vier Online Auktionshäusern) wurden Betreiber von Online-Handelsplattformen zu ihrer Wahrnehmung des Problems Online-Betrug befragt. Mit der kleinen Fallzahl sind die Ergebnisse der Studie nicht repräsentativ, sie liefern vielmehr Hinweise und Ansatzpunkte und dienen dazu, Lösungen für adäquate Gegenreaktion gegen das Phänomen Betrug im Online-Handel zu entwickeln.

Drei wesentliche Tendenzen konnten isoliert werden:

1. Die Befragung zeigte, dass eine digitale Authentifizierung zur Steigerung der Sicherheit im Online-Handel eine hervorragende Verbesserungsmöglichkeit bildet. Sowohl für die Nutzer als auch für sich selbst halten die Betreiber eine Überprüfung der jeweiligen Identität für die effektivste Sicherheitsmaßnahme. Doch bislang fehlt hier aus Sicht der Betreiber noch eine komfortable, kostengünstige und vor allen Dingen sichere Lösung, die für jeden Verbraucher einfach anzuwenden ist.

2. Eine weitere Möglichkeit, sich vor Betrügern im Online-Handel zu schützen, sehen die Betreiber auch in der Anpassung der Datenschutzbestimmungen. Wünschenswert aus Sicht der Betreiber wäre es, Kundendaten bereits während einer Transaktion frühzeitig mit einer entsprechenden Datenbank abzugleichen. Kreditkartenunternehmen können diese Art der Verhaltensmustererkennung bereits heute durchführen und so möglichen Betrug frühzeitig erkennen, unterbinden und sich selbst aktiv schützen.

3. Die Erfahrung der Betreiber zeigte auch, dass die Internetnutzer über die erforderlichen Sicherheitsmaßnahmen im Internet zutreffend und besser informiert sein müssen.

Diese Wahrnehmung wird von einer weiteren Studie von tns emnid im Frühjahr 2005 bestätigt. Bei der repräsentativen Studie „Sicherheit im Internet“, in deren Zentrum die Internetnutzer standen, schätzen 63 % der Befragten das Internet als unsicher ein. Dennoch werden technische Sicherheits- und persönliche Verhaltensmaßnahmen oft nicht wahrgenommen, obwohl diese bekannt sind. Es besteht also eine Diskrepanz zwischen technischer Prävention und persönlicher Risikowahrnehmung bei den Nutzern. Zum gleichen Ergebnis kam auch die im Herbst 2004 in Auftrag gegebene Studie des Bundesamtes für Sicherheit in der Informationstechnik.

Nach Einschätzung der befragten Unternehmen werden Betrugsdelikte nur selten zur Anzeige gebracht. Die Händler selbst leiten Betrugsfälle erst ab einer gewissen Schadenshöhe an die Behörden weiter, da der Arbeits- und Verwaltungsaufwand sehr hoch ist. Fehlgeschlagene Betrugsversuche werden prinzipiell nicht gemeldet. Dabei gehen die Betreiber davon aus, dass die Behörden prinzipiell kompetente Ansprechpartner in Sachen Strafverfolgung, jedoch überlastet sind. Offenbar – so die Befragten - schrecken auch viele private Nutzer aus Angst vor dem bürokratischen Aufwand vor einer Strafverfolgung zurück, wenn sie Opfer eines Online-Betrugs geworden sind.

5. Handlungsempfehlungen

Die Projektgruppe Effektive Betrugsbekämpfung hat zu Beginn ihrer Beratungen einen Katalog über mögliche Maßnahmen aufgestellt.[16] Die Recherche hat ergeben, dass einige der genannten Maßnahmen bereits umgesetzt werden konnten. Im Rahmen der Arbeit der Projektgruppe Effektive Betrugsbekämpfung konnten letztlich unter Einbeziehung der Ergebnisse der Befragung fünf große Handlungsbereiche identifiziert werden, die auch in Zukunft für die Eindämmung von Betrug im Online-Handel eine entscheidende Rolle spielen werden:

1. Verbraucheraufklärung
2. Sicherheitsstandards
3. Effektivierte Strafverfolgung
4. Nationale Kooperation
5. Internationale Kooperation

Im Bereich dieser Felder erachtete die Projektgruppe folgende zwei Handlungsfelder als vordringlich:

a) Die diagnostizierte Diskrepanz zwischen dem Wissen der Verbraucher um Risiken im Internet und mögliche Abhilfe einerseits und der persönlichen Risikowahrnehmung und dem daraus resultierenden Handeln andererseits muss verringert werden. Hier könnte ein Informations- und Lernangebot helfen, dass die Nutzer breit erreicht und leicht verständliche Informationen interaktiv anbietet. Konzeption und Umsetzung könnte die Wirtschaft und Experten im Bereich Kriminalprävention im Internet wie zum Beispiel Vertreter von Präventionsgremien und Ermittlungs- und Strafverfolgungsbehörden leisten.

b) Eine bundesweite Arbeitsgruppe sollte eingerichtet werden, in der die mit der Prävention von Betrugsdelikten befassten Ermittlungs- und Strafverfolgungsbehörden und die Wirtschaft Informationen und Erfahrungen austauschen und so zu einer besseren Prävention von Betrugsdelikten beitragen.

Die Projektgruppe Effektive Betrugsbekämpfung hat mit dem vorliegenden Überblicks-Bericht zum Sachstand der Betrugsbekämpfung im Online-Handel und der Formulierung von Handlungsempfehlungen ihre Ziele erreicht. Im Rahmen der Initiative D21 werden derzeit die Möglichkeiten einer künftigen praktischen Umsetzung ausgewählter Maßnahmen zur effektiveren Betrugsbekämpfung geprüft.

16 Anhang 1

Anhang 1
Vorschläge für einen Maßnahmen-Katalog

1. Verbesserung der Zusammenarbeit bei der Bekämpfung des Betrugs im Internet von Verwaltung, Wirtschaft, Strafverfolgungsbehörden
   Maßnahme: Etablierung einer ständigen Arbeitsgruppe mit den Instituten Wirtschaft, Polizei und Strafverfolgung (Beispiel: Heppenheim)

2. Sensibilisierung der Nutzer und der Unternehmen für eine sicherheitsbewusste Nutzung des Internets
   Maßnahme: Internetportal zum Thema Sicherheit

3. Anbieten der nach dem Stand der Technik sicheren Bezahl- und Abrechnungssysteme mit kundenorientierten transparenten Geschäftsabläufen
   Maßnahme: Einführung einer Arbeitsgruppe Banken, Handel, IT und Strafverfolgung zur Entwicklung neuer Sicherheitsstandards

4. Stärkung der Kompetenz von Internetnutzern für eine verantwortungsvolle Abwicklung im elektronischen Handel und bei Bezahlvorgängen im Internet
   Maßnahme: Erstellung eines Internetportals mit Warnmeldungen (möglich wäre eine Ausdehnung gemäß www.Kartensicherheit.de, s.o.)

5. Schadensreduzierung durch zeitnahe Öffentlichkeitsarbeit der Verantwortungsträger (Provider, Anbieter, Versandhandel, Polizei etc.)

   Je schneller Missbrauchsfälle bekannt werden, umso größer ist die Chance, Schäden zu vermeiden. Der Kunde muss wissen, was im Schadensfalle zu tun ist und vor welchen Kriminalitätsphänomenen er sich schützen sollte.
   Maßnahme: aktive Förderung Sperr e.V und Internetportal zum Thema Sicherheit

6. Entwicklung technisch verbindlicher Standards zur Qualitätssicherung des Warenhandels im Internet und Einsetzen unabhängiger Prüf- und Kontrollinstanzen

   Es gibt zu viele unterschiedliche Sicherheitsfeatures, die von dem „normalen" User nicht verstanden werden. Forderung nach der „einfachen" Darstellung der Sicherheitsfeatures der Händler und Institute zur Erreichung eines Maximums an Sicherheitsstandards. Zielrichtung müsste hier ein „TÜV" für den Warenhandel im Internet sein.
   Maßnahme: Arbeitsgruppe Banken, IT, Handel, Strafverfolgung

7. Initiierung einer öffentlichkeitswirksamen Kampagne mit dem Ziel der Vertrauensbildung und -stärkung für den eCommerce
   Maßnahme: Kampagne der Bundesregierung - Kompetenzstärkung aller Beteiligten

8. **Maßnahme:** Weiterentwicklung der bestehenden länderübergreifenden Kontaktnetze

9. Effektive Prozessdokumentation und effizientes Risikomanagement
   Maßnahme: Präventive Beurteilung des Zahlungsverhalts eines Neukunden durch Einsatz von Scoringsystemen (z. B. große Anbieter: SCHUFA, InfoScore); Auffällige Bestellungen, die nicht in den normalen Bestellablauf passen („30 Satellitenschüsseln nach Weißrussland") an einen Sachbearbeiter aussteuern; Erstkunden aus Risikogruppen bei der Erstbestellung nur per Nachnahme beliefern – erst bei folgenden Lieferungen andere Zahlungsarten anbieten; Genaue Bezeichnung inkl. Seriennummern der gelieferten Ware sowie genaues Gewicht des Pakets und Identität des Packers elektronisch erfassen; Regelmäßige unternehmensinterne Überprüfung des Bestellvorgangs auf der Basis der festgestellten Betrugsfälle.

Literatur

1. Bundesamt für Sicherheit in der Informationstechnik (BSI) / TNS Emnid (2005): Bürger zu sorglos im Internet. Siehe unter: http://www.bsi.de/presse/pressinf/270105ohn_Virensch.htm

2. Bundeskriminalamt: Lagebild IuK-Kriminalität Bundesrepublik Deutschland 2003. Siehe unter: http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_kriminalitaet_2003.pdf

3. Initiative D21 e.V. / AOL Deutschland / TNS Emnid (2005): Sicherheit im Internet. Siehe unter: http://www.alle.de/transfer/downloads/MD518.pdf

4. eTForecasts, Pressemitteilung vom 27.09.2004. Siehe unter: http://www.etforecasts.com/pr/pr904.htm

5. (N)ONLINER Atlas 2005, TNS Infratest und Initiative D21 e.V.. Siehe unter: http://www.nonliner-atlas.de/

6. Polizeiliche Kriminalstatistik 2004. Siehe unter: http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Broschueren/2005/Polizeiliche__Kriminalstatistik__2004__de.html

7. Postbank / Europressedienst Research: eCommerce 2004 – Strukturen und Potenziale des eCommerce in Deutschland aus Kunden- und Händlersicht, November 2004. Siehe unter: http://www.postbank.de/Datei/fk_ecommerce_studie,0.pdf

8. Statistisches Bundesamt: Informationstechnologie in Unternehmen und Haushalten 2004, Wiesbaden 2005. Siehe unter: http://www.destatis.de/informationsgesellschaft/d_home.htm

Links

1. Bundesamt für Sicherheit in der Informationstechnik (BSI). Siehe unter: www.bsi.bund.de

2. BSI für Bürger. Onlineportal des Bundesamtes für Sicherheit in der Informationstechnik zum Thema Sicherheit im Internet. Siehe unter: www.bsi-fuer-buerger.de

3. Deutschland sicher im Netz. Initiative von D21 e.V., AOL Deutschland und TNS Emnid. Siehe unter: www.sicher-im-netz.de

4. ProPK Online. Vorbeugungsprogramm der Polizei im Internet. Siehe unter: http://www.polizei-beratung.de

5. Sicherheit im Internet. Initiative des Bundesministeriums für Wirtschaft und Arbeit sowie des Bundesministeriums des Innern. Siehe unter: www.sicherheit-im-internet.de