dp special

Supplement der Zeitschrift Deutsche Polizei Nr. 4/98



INTERNET

Die virtuelle Welt des Verbrechens

Zwischen drei und fünf Millionen Personen in der Bundesrepublik benutzen das Internet. Internationale Benutzerzahlen sind nicht einmal zu schätzen. Im Internet wird täglich eine Datenmenge von mehr als 300 Gigabyte übertragen, was einer halben Million Bücher mit je 250 Seiten entspricht. In 184 Ländern der Erde bestehen Zugänge zum Internet. Zum Vergleich: INTERPOL hat 177 Mitgliedsstaaten. Internet – das für Laien wie auch für viele Fachleute schier undurchschaubare Kommunikationsnetz, mit dem man Tag und Nacht bis in die letzten Winkel der Welt Informationen und Daten sammeln, austauschen und abrufen und sonst allerlei Nützliches, Unterhaltsames anstellen kann, ist auch für die Polizei zum Thema geworden. Mit den Werkzeugen, die die virtuelle Welt bereit hält, kann großer Schaden angerichtet werden.

Von Thomas Hartung

Dies ist auch ins öffentliche Bewußtsein gedrungen, spätestens seit man weiß, daß Internet dazu mißbraucht wird, Kinderpornographie zu verbreiten. Doch der kriminelle Mißbrauch der aus der modernen Welt nicht mehr wegzudenkenden Kommunikationseinrichtung Internet hat noch ganz andere Dimensionen. Die seit Jahren bekannten, teils amüsierenden teils erschreckenden Berichte über das Geschick von Hakkern, verbotenerweise in Datennetze einzudringen, sind nur einige wenige von vielen Beispielen über die Gefahren, die durch kriminelle Machenschaften mit dem Internet drohen.

Geschichte und Technik des Internet

In den Sechziger Jahren begann das amerikanische Verteidigungsministerium damit, ein Projekt zu fördern, das die militärische Nutzbarkeit von Computernetzwerken verbessern sollte. Es war erkannt worden, daß die Landesverteidigung von miteinander verbundenen Computersystemen abhängig war. Es mußte also ein System entwickelt werden, das auch bei Ausfall von einzelnen Verbindungen, Leitungen oder Netzknotenpunkten die Kommunikationsfähigkeit bzw. die Verbindung von Militärrechnern sicherte.

Mit der Entwicklung der benötigten Netzwerktechnik beschäftigten sich mehrere amerikanischen Universitäten. Hierbei bekam das so entstehende Netz neben seiner militärischen auch eine wissenschaftliche Funktion als Verbindung zwischen einzelnen Wissenschaftseinrichtungen.

Der Autor



Thomas Hartung (27), Kriminaloberkommissar beim Bundeskriminalamt. Sachbearbeiter im Referat OA 34 (Wirtschafts- und I.u.K.-Kriminalität), Fachgebiete Internet und Telefonkartensimulatoren.

IMPRESSUM:
dp-special zur Ausgabe Deutsche Polizei Nr. 4 · 47. Jahrgang 1998 · Fachzeitschrift und Organ der Gewerkschaft der Polizei

Herausgeber:
Gewerkschaft der Polizei, Forststraße 3a, 40721 Hilden, Telefon (0211) 7104-0, Telefax (0211) 7104-222

Redaktion:
Adalbert Halt (verantwortlich), Rüdiger Holecek, Gewerkschaft der Polizei, Pressestelle, Forststraße 3a, 40721 Hilden, Telefon (0211) 7104-101 bis 105, Telefax (0211) 7104-138
E-Mail:
CompuServe: 106655,542
Internet: 106655.542@compuserve.com

Grafische Gestaltung, Layout und Titel:
Rembert Stolzenfeld

Verlag & Anzeigenverwaltung:
VERLAG DEUTSCHE POLIZEI-LITERATUR GMBH, Forststraße 3a, 40721 Hilden
Telefon (0211) 7104-183
Telefax (0211) 7104-174

Anzeigenleiter:
Michael Schwarz
Es gilt die Anzeigenpreisliste Nr. 25 vom 1. Januar 1997

Herstellung:
L.N. Schaffrath GmbH & Co.KG, Hartstraße 4-6, 47608 Geldern, Telefon 02831-396-0, Telefax 02831-89887

Um den universitären Bereich mit Studenten und Professoren von der Landesverteidigung abzutrennen, zog sich das Militär in den achtziger Jahren aus dem Internet zurück und richtete eigene, vom Internet abgetrennte Netze ein. Das Internet entwickelte sich verstärkt zu einem nichtkommerziellen Netzwerk, als Verbindung von Wissenschaftseinrichtungen in aller Welt.

Seit der Einführung des World Wide Web (WWW) als grafische Benutzeroberfläche im Jahr 1993, wandelte sich das Internet nun zu einem weltweiten, kommerziellen und nichtkommerziellen Computernetzwerk, das jedem Interessierten eine Vielzahl von Möglichkeiten bietet.

Zwischen miteinander kommunizierenden Rechnern besteht keine direkte Verbindung. Zu übertragende Daten werden in Pakete zerteilt, die dann unterschiedlichste Wege nutzen (paketorientierte Übermittlung). Dies geschieht in Abhängigkeit von der Verfügbarkeit und Geschwindigkeit der unterschiedlichen Leitungen des Internet. Die Datenpakete werden mit Absender und Empfängeradressen versehen. Die Übermittlung von Daten ist grundsätzlich nicht verschlüsselt, sondern offen und mitlesbar.

Für das Netzwerk sind keine zentralen technischen Systeme notwendig. Rechner können an einer beliebigen Stelle ins Netzwerk eingehängt werden.

Da alle am Internet beteiligten Geräte eindeutig adressiert sein müssen, um ansprechbar zu sein, werden für jedes Gerät Nummern, die sogenannten IP-Nummern, vergeben. Da diese ein für Menschen schlecht merkbares Zahlenformat haben, z.B. 194.77.91.35, und häufig gebraucht werden, um einen Rechner im Internet anzusprechen (z.B. den des BKA), werden sie in Buchstabenkombinationen übertragen (z.B. www.bka.de für 194.77.91.35). Dieser Name beinhaltet am Ende eine sogenannte Länderkennung. IP-Nummern und die dazugehörigen Namen werden in jedem Land zentral von einer Stelle vergeben. Dies geschieht in Deutschland durch das DENIC, eine Genossenschaft die von großen deutschen Internet-Providern gemeinsam betrieben wird.

Daß sich die Internet-Technologie weiter durchsetzen wird, zeigt sich insbesondere daran, daß immer mehr firmeninterene Netzwerke als Intranet-Systeme aufgebaut werden. Hier finden die Browserprogramme des WWW Verwendung und Daten werden mit den technischen Standards des Internet übertragen. Die Unterschiede zwischen dem eigenem Rechner, dem Intranet und Internet werden sich zukünftig weiter verwischen.

Zugang zum Internet bieten Internet-Provider. Onlinedienste (z.B. T-Online, AOL, Compuserve) bieten neben dem Zugang zum Internet auch ein eigenes, nur für ihre Kunden zugängliches, Angebot. Die hier angebotenen Dienste sind weitestgehend mit denen im Internet identisch. Der Zugang wird in der Regel über Daten oder Telefonleitungen realisiert. Neben den Telefongebühren entstehen entweder pauschale Benutzungskosten zwischen 10 DM und 50 DM im Monat oder Gebühren, die von der Onlinezeit oder den übertragenen Datenmengen abhängen.

Weitere Möglichkeiten, auf das Internet zuzugreifen, befinden sich inzwischen in den sogenannten Internet-Cafes, als „Lockangebot“ in Geschäften, in dafür vorgesehenen Räumen an Universitäten oder Hochschulen, in Firmen oder Hotelempfangshallen, in Spielotheken und an vielen anderen Plätzen.

Für den Privatbereich benötigt man einen Personal Computer mit Modem oder ISDN-Karte, um den Zugang zum Provider über das Telefonnetz herzustellen. Es befinden sich Systeme in der Erprobung, die über andere Wege (Kabelfernsehnetz, Funkübertragung, Satellitenempfang) die Verbindung zum Internet herstellen. Als Endgeräte sollen auch Fernseher oder spezielle Internet-Terminals eingesetzt werden.



Per Maus-Klick um die ganze Welt.

Die Dienste des Internet und die Möglichkeiten ihres Mißbrauchs

Die verschiedenen Dienste des Internet gehen oftmals ineinander über und ständig werden neue entwickelt. An den einzelnen Diensten lassen sich verschiedene kriminelle Erscheinungsformen oder Nutzungsmöglichkeiten des Internet darstellen.

Über Datenleitung (TELNET) ist die vollständige Benutzung aller Funktionalitäten eines örtlich entfernt stehenden Rechners möglich. TELNET ist die schier unerschöpfliche Spielwiese für Hacker und Datenspione. Kaum mehr zu überschauen sind die Berichte über Angreifer, die über Datenleitungen in fremde Rechner eingedrungen sind. Angriffsziele waren vertrauliche Daten, z.B. Kundeninformationen oder Kontodaten. In der Folge wurden die Daten häufig genutzt, Geld zu erpressen, wobei mit der Veröffentlichung der Daten gedroht wurde. Daß vertrauliche Kontoinformationen den von der Erpressung Betroffenen zum Beispiel im Fall eines Schwarzgeldtransfers den Angstschweiß auf die Stirn treiben können, mag nachvollziehbar sein.

Die Science-Fiction-Spielart, wonach es möglich ist, eine Persönlichkeit durch Zugriff auf Datennetze völlig auszulöschen, ist heute durchaus in den Bereich der Realität gerückt. Kontoführung, Einwohnermeldeamt, Krankenkassenkarte – alles Datensammelstellen, die unser Leben bestimmen und die aufs engste mit der Computertechnik verbunden sind.

Ein weiteres, noch brisanteres Szenario: Der Begriff „Information Warfare“ beschreibt eine Möglichkeit, die Kriege bisherigen Zuschnitts alsbald ablösen könnte. Über den kriminellen Zugriff auf Daten können ganze Länder oder ihre Wirtschaftsunternehmen ausgeschaltet, zumindest aber behindert werden. In bestimmten Wirtschaftsbereichen kann der Ausfall eines Computers zum Konkurs einer ganzen Firma führen. Überall dort zum Beispiel, wo mit Geld gehandelt wird, würde ein Stillstand der Datenverarbeitung zu irreparablen Schäden führen.

Die Landesverteidigung ist ohne Computertechnik nicht mehr denkbar. Im Bereich der Spionage ist der Zugriff auf fremde Computer von höchstem Interesse, und die Ausspähung eines Mitbewerbers um den Verkauf eines Schnellzugsystem an Südkorea oder der Diebstahl von Daten über ein chemisches Patent einer konkurrierenden Firma können weitreichende Folgen haben.

Austausch raubkopierter Software

Mittels Softwarearchiven (FTP, FSP) können Dateien zwischen zwei Rechnern online verschickt (upload) oder abgerufen (download) werden. Es gibt im Internet eine Vielzahl von Rechnern (FTP-Server), auf denen Software vorgehalten wird. Auf diese Rechner kann über das Internet zugegriffen werden. Es ist möglich, auf dem eigenen Rechner (zumindest temporär) Dateien anzubieten. Dieser Dienst wird von großen Softwareherstellern zur Verbreitung von Ergänzungen (z.B. Fehlerbereinigungen) ihrer Software benutzt. Desweiteren wird Shareware oder Freeware über solche Rechner vermarktet. Komplette Programmpakete werden in der Regel nicht auf diesem Weg vertrieben, da hierfür die Übertragungsdauer momentan noch zu lange dauert. Mit zunehmender Bandbreite im Internet wird auch dies möglich werden.

Mit Hilfe dieses Dienstes können raub-kopierte Software ausgetauscht oder beweisrelevante Daten auf fremden Rechnern abgelegt werden. Weiterhin können sie zur Begehung vieler Staatsschutzdelikte benutzt werden (z.B. durch Bereitstellung von verbotenem Propagandamaterial auf Rechnern, die sich im Ausland befinden). Auch können über diese Dienste Schadensprogramme (z.B. Computerviren), versteckt in anderen Dateien, verbreitet werden.

Nachrichtenaustausch auf „Schwarzen Brettern“ (USENET)

Dieser Dienst ermöglicht Benutzern des Internet, in bestimmten Nachrichtengruppen (Newsgroup) Mitteilungen zu verschiedenen Themengebieten (z.B. technische Probleme, Gespräche über Gesundheitsprobleme etc.) zu hinterlassen. Man unterscheidet zwischen moderierten und unmoderierten Newsgroups. Im Gegensatz zu den unmoderierten, bei denen der Autor entscheidet, daß seine Mitteilung in einer Newsgroup erscheint, trifft in einer moderierten Newsgroup ein Moderator die Auswahl, welcher Beitrag aufgenommen wird oder nicht.

Die Mitteilungen einer Newsgroup sind dem Benutzer zugänglich, der die betroffene Newsgroup anwählt. Es besteht die Möglichkeit, die Nachrichten mit und ohne Absenderangabe in den Newsgroups zu plazieren. In Verbindung mit den Nachrichten können auch Dateien (z.B. Bild- oder Tondateien) weitergegeben werden.

Im Internet wurde eine Vielzahl von Rechnern (Newsservern) eingerichtet, auf denen eine vom Betreiber des Servers ausgewählte Anzahl von Newsgroups angeboten wird. Diese Server sind entweder für alle Benutzer des Internet oder nur für bestimmte zugäng-

lich. Die Newsserver gleichen in einem automatischen Prozeß ständig den Inhalt von gemeinsam geführten Newsgroups ab und kopieren Veränderungen. Populäre Newsgroups werden auf einer Vielzahl von Newsservern geführt. Die Nachrichten innerhalb einer Newsgroup werden aufgrund des begrenzten Speicherplatzes nach einer bestimmten Zeit gelöscht.

Es gibt ca. 30.000 verschiedene Newsgroups im Internet, wobei kein Newsserver bekannt ist, der alle Newsgroups führt und somit keine genaue Zahl festzulegen ist. Die Newsgroups werden zur Verbreitung von verbotenen Schriften und Bilder aller Art (z.B. kinderpornographische Darstellungen) benutzt. Dies geschieht einerseits über Newsgroups, die thematisch für diesen Bereich eingerichtet wurden (z.B. alt.binaries. pictures.preteen). Es kann andererseits auch jede andere unmoderierte Newsgroup genutzt werden.

In den Newsgroups werden Informationen zu Staatsschutzdelikten, Hacking, Softwarepiraterie oder kinder- und tierpornografische Darstellungen verbreitet.

Elektronische Post (Email)

Mit Hilfe dieses Dienstes ist der schnelle, weltweite Austausch von Nachrichten möglich. Diese Nachrichten werden an eine bestimmte Adresse oder einen bestimmten Empfängerkreis versandt, so daß im Unterschied zu den Newsgroups nicht jeder beliebige Nutzer des Internet die Mitteilungen mitlesen kann. Ferner können sogenannte Mailinglisten erstellt werden, mit denen elektronische Rundschreiben verschickt werden. In der Regel erhält ein Kunde von seinem Provider, der ihm den Zugang zum Internet eröffnet, eine Email-Adresse (z.B. mustermann@t-online.de). Für diesen Dienst betreibt der Provider einen Rechner (Email-Server) auf dem zu der Email-Adresse ein Postfach eingerichtet wird. Der Kunde kann also, wenn er aktuell mit dem Provider verbunden ist, auf diesem Server die für ihn eingegangene Post abrufen, bzw. bei dieser Gelegenheit Nachrichten an andere schicken. Neben dieser „Standardmöglichkeit" gibt es auch verschiedene Angebote, ein solches Postfach bei einem Anbieter im WWW zu betreiben.

Die Nachrichten können mit verschiedenen, meist frei erhältlichen Verschlüsselungsprogrammen so bearbeitet werden, daß sie nur der eigentliche Empfänger lesen kann. Es besteht die Möglichkeit, Nachrichten ohne nachvollziehbare Absenderadresse zu verschicken. Für nicht verschlüsselt versandte Emails besteht die Gefahr, daß sie von unberechtigten Personen im Internet mitgelesen werden können. Die dadurch gewonnenen Informationen sind eventuell im Zusammenhang mit (Wirtschafts-) Spionage oder anderen Delikten von Interesse.

In einem Erpressungsfall nutzte der Täter ein anonymes Postfach im Internet, um Kontakt mit dem Opfer und der Polizei aufzunehmen. Er hatte die Möglichkeit, von jedem Rechner, der ans Internet angeschlossen ist, auf diese Daten zuzugreifen. Zur Eröffnung des Postfachs nutzte er falsche Personalien. Die Ermittlungen konnten nur dadurch geführt werden, daß jedesmal, wenn er auf sein Postfach zugriff, festgehalten wurde, von welchem Rechner im Internet aus zugegriffen wurde. Die Feststellung, wer diesen Rechner zum fraglichen Zeitpunkt benutzt hat, gestaltete sich äußerst schwierig.

Die anonymen Email-Postfächer im Internet stellen einen toten Briefkasten dar, der nicht örtlich gebunden ist. Er kann von jedem Punkt der Erde aus – sofern eine Internet-Verbindung besteht – aufgerufen und geleert werden. Eine Observation ist nur unter sehr erschwerten Bedingungen möglich.

Telefonieren im Netz (Internet-PHONE)

Da die Benutzung des Internet mit wesentlich geringeren Gebühren verbunden ist als die Benutzung des Telefonnetzes, werden verschiedene Möglichkeiten entwickelt, über das Internet zu telefonieren. Hierfür werden Sprachinformationen in Datenpakete umgewandelt und beim jeweiligen Gesprächspartner wieder in Sprachausgabe umgesetzt. Dieses System ist momentan noch nicht ausgereift und wird von verschiedenen Faktoren erschwert.

So sind die Datenübertragungsraten im Internet noch nicht schnell und stabil genug, um ein unterbrechungsfreies Gespräch, wie man es von normalen Telefon gewohnt ist, zu gewährleisten. Außerdem müssen beide Gesprächspartner aktuell ans Internet angeschlossen sein, um ein Gespräch zu beginnen. Deshalb gibt es verschiedene Projekte, die Datenleitungen des Internet zu nutzen, über spezielle Rechner aber eine Verbindung ins normale Telefonnetz herzustellen. Es ist auch denkbar, Computer in einen „Standby-Betrieb" zu versetzen, so daß sie bei einem ankommenden Ruf gestartet werden. Durch zunehmende Leitungskapazitäten im INTERNET bzw. die Möglichkeit, gegen Gebühr Leitungskapazitäten gezielt zu reservieren, werden auch zunehmend unterbrechungsfreie Telefonate möglich werden. Neben den günstigen Gesprächsgebühren zählt als weiterer Vorteil der INTERNET-Telefonie die Möglichkeit, auf einfach-

stem (Software gestütztem) Weg Gespräche zu verschlüsseln. Daß diese Kommunikationsmöglichkeit auch von Straftätern vermehrt genutzt werden, versteht sich von selbst.

Online Diskussionsforen (IRC)

Dieser Dienst ermöglicht die Teilnahme verschiedener User des INTERNET an moderierten oder unmoderierten Diskussionsforen. Es werden in den einzelnen, thematisch sortierten Foren („Chatrooms"), Textbotschaften in Echtzeit ausgetauscht. Es besteht die Möglichkeit, nur einen bestimmten Kreis von Usern an einer Diskussion teilnehmen zu lassen. Während eines Dialogs können Dateien (z.B. Bilder) ausgetauscht werden.

Es bestehen eine Vielzahl von Chatrooms, die sich mit sexuellen Themen beschäftigen. Sie werden insbesondere im Bereich Kinderpornographie zum Kennenlernen von Gleichgesinnten genutzt, um dann in einen regen Materialtausch einzusteigen. Schon ein kurzer Aufenthalt in Foren führt unweigerlich zu Angeboten aus dem schlüpfrigen Bereich. Es ist davon auszugehen, daß hier Kontakte angebahnt werden, die sich dann über den Austausch von Bildern und Adressen fortsetzen.

Die Möglichkeit zur anonymen Teilnahme an Dialogen in einem Chatroom macht ein Herantasten an die Szene möglich, ohne daß man für strafbare Handlungen persönlich haftbar gemacht werden kann. Die Polizei hat aufgrund der vielen verschiedenen Chatrooms sowie der Verwendung von Fakes (Falsch- oder Spitznamen) kaum Ermittlungsansätze.

Erschwerend kommt der Umstand hinzu, daß eine Vielzahl von Teilnehmern in den Chatrooms nur einfach mal ausprobieren wollen, was möglich ist, und den von ihnen getroffenen Aussagen kein reeller Sachverhalt zugrunde liegt. Extreme Beispiele sind Angebote über sadistischsten Kindesmißbrauch bis hin zum Mord, die oft als „Spaß" oder Test verstanden werden, aber nicht wirklich geplant sind.

Grafische Benutzeroberfläche (World Wide Web)

Dieser Service bietet eine grafische Oberfläche, mit der die Nutzung der oben beschriebenen Dienste stark vereinfacht wird oder neue Nutzungsmöglichkeiten zur Verfügung gestellt werden. Die Einführung dieses Dienstes im Jahr 1993 hat die explosionsartige Verbreitung des Internet eingeleitet. Auch die fortschreitende Kommerzialisierung des Internet wird durch diesen Dienst vorangetrieben.

So sind verschiedenste Anbieter im World Wide Web (WWW) vertreten, die sich präsentieren, oder bei denen der Einkauf von Waren möglich ist. Auch für Privatpersonen besteht die Möglichkeit, sich hier vorzustellen. So bieten viele Provider ihren Kunden einen Speicherplatz für eine Präsentation an. Andere Anbieter bieten dies gegen Gebühr an oder plazieren zur Finanzierung Werbung auf den Seiten eines privaten Nutzers. Da kein zentrales Verzeichnis der Inhalte des WWW besteht, werden von verschiedenen Anbietern sogenannte Suchmaschinen betrieben, die es erlauben, nach bestimmten Begriffen im WWW zu suchen. Entsprechende Suchmaschinen werden auch für die Newsgroups angeboten.

Gerade im WWW ist die Sexualität in allen möglichen Spielarten ein Hauptthema. Dafür sprechen z.B. die Statistiken über die von Benutzern abgefragten Suchbegriffe, die von den Suchmaschinen erstellt werden. Hierbei spielen hauptsächlich Begriffe aus dem sexuellen Bereich eine Rolle. (Ein Beispiel hierfür ist z.B. die Statistik der deutschen Suchmaschine „Kolibri", die im WWW unter der Adresse „http://www.kolibri.de/cgi-bin/top.ksh" abzufragen ist). Nach den Gesetzen von Angebot und Nachfrage dürfte die Suche nach solchen Inhalten auch von Erfolg gekrönt sein.

Bei dem verbreiteten verbotenen Pornographien handelt es sich häufig um ein bereits existentes Material. Bisher wurde kein Fall bekannt, in dem Material speziell deshalb hergestellt wurde, um die Nachfrage aus dem Internet zu befriedigen. Personen, die sonst nie damit in Kontakt kommen würden, nutzen die vereinfachten und anonymen Zugriffsmöglichkeiten des Internet, um ihre Neugier (und manchmal ihre verborgenen sexuellen Phantasien) zu befriedigen.

Ob durch die erhöhte Nachfrage auch irgendwann neues Material mit dem Ziel der Präsentation im Internet erstellt wird, ist bisher nicht abzusehen. Die Möglichkeiten der Computertechnik, die es erlauben, ein tatsächliches Geschehen zu simulieren und auf diese Weise täuschend echt wirkende Bilder zu erstellen, werden verstärkt genutzt werden.

Es gibt bereits erste Fälle, in denen die interaktiven Möglichkeiten des Internet gezielt genutzt wurden. In einem Fall wurde eine Videokamera auf eine Frau gerichtet. Verschiedene Benutzer des Internet gaben Anweisungen, was die Frau tun sollte. Die Bilder wurden zeitgleich auf einer Seite im WWW gezeigt.

Eine neue Technik breitet sich gegenwärtig von Japan aus über das Internet aus. Mit Hilfe eines Softwareprogramms (FL-Mask) ist es möglich, bestimmte Bereiche eines Bildes mit einem verdeckenden Balken zu versehen. Die Bil-



Ermittlung am Bildschirm: Suche nach den Köpfen im Hintergrund. Fotos(2): H. Wesseling

der können dann im Internet verbreitet werden und zeigen damit kein Geschehen mehr, welches als strafrechtlich relevant zu bezeichnen wäre. Der Empfänger der Bilder kann mit Hilfe der Software die Balken entfernen und zum Originalbild zurückkehren.

Der Phantasie, wie das Internet kriminell genutzt wird, sind keine Grenzen gesetzt: Verbreitung extremistischer Propaganda, Aufrufe zu verbotenen Versammlungen, verbotenes Glücksspiel, betrügerisches Anbieten von Waren und Dienstleistungen zur Erlangung von Kreditkartennummern oder Geldbeträgen oder betrügerische Geldanlageangebote, Urheberrechtsverletzungen, Informationen zur Herstellung synthetischer Drogen oder zum Verkauf von in Deutschland verbotenen Medikamenten. In diesem Fällen erfolgt Bestellung und Bezahlung direkt über das Internet.

Die Dienste des Internet, die in erster Linie mit Kommunikation zu tun haben (Email, Newsgroup, Internet-Telefonie, IRC etc.), sind auch für Straftäter nutzbar und durch ihre Vorteile (einfachste Verschlüsselung, erschwerte Nachvollziehbarkeit) für sie von Interesse. Die Erfahrung zeigt, daß Straftäter häufig zu den ersten Nutzern einer neuen Technologie gehören. Ein gutes Beispiel ist z.B. der Einsatz von Handys.

Finanzdienstleistungen im Internet

Im Zuge der zunehmenden Bedeutung des Internet als kommerzielles Medium wird auch verstärkt darüber nachgedacht, wie verschiedene Formen der Finanzdienstleistungen in dieses Medium integriert werden können. Es geht hier zum einen darum, Bezahlmöglichkeiten für bestimmte Inhalte des Internet zu schaffen, andererseits aber auch die Internationalität des Netzes für Finanztransaktionen jeglicher Art zu nutzen.

Im Internet gibt es eine Vielzahl von Angeboten aus dem Bereich der Finanzwelt. Dazu gehören ständig aktualisierte Fachinformationen, Börsenkurse, Versicherungsmakler, Banken, Broker, Einkaufsmöglichkeiten, etc. Diese Angebote beginnen meist mit einer reinen Informationsdarstellung. In der nächsten Stufe besteht dann im Rahmen der Dienste des Internet die Möglichkeit der Kontaktaufnahme zwischen Anbieter und Kunden, um finanzielle Transaktionen direkt über das Internet durchzuführen.

Diese Transaktionen müssen bestimmten Sicherheitsanforderungen genügen, die durch unterschiedliche Schutzmechanismen bei den einzelnen Konzepten realisiert werden.

Kreditkartennummern nicht sicher

Bisher wird für Bezahlungsvorgänge im Internet häufig eine Abrechnung unter Angabe der Kreditkartennummer benutzt. Dieses Verfahren ist aber durch die leichte Ausspähbarkeit der Daten im Internet in keiner Weise sicher.

Es ist für den technisch einigermaßen versierten Angreifer möglich, diese Daten mitzulesen und für eigene Zwecke zu mißbrauchen.

Es werden Transaktionsverfah-

ren angeboten oder noch entwikkelt, die bestimmte Sicherheitsstandards erfüllen. Hierbei werden z.B. Verfahren eingesetzt, bei denen eine verschlüsselte Übertragung der Kreditkartennummer stattfindet oder die Abrechnung über eine weitere Firma stattfindet.

Für den Bereich der Bankgeschäfte kommen verschiedene Homebanking-Verfahren zum Einsatz. Bei diesen werden zur Absicherung der Transaktionen soft- oder hardwareorientierte Verschlüsselungsverfahren eingesetzt. Desweiteren kommen PIN und TAN zum Einsatz. Im Jahr 1997 wurde von den deutschen Banken der neue Standard für das Homebanking im Internet, HBCI (Homebanking Computer Interface) verabschiedet, so daß man hier mit einer gewissen Vereinheitlichung der Abläufe rechnen kann.

Die Geldtransaktion über Kreditkartennummer oder Bankgeschäft hat aber einige gravierende Nachteile. So ist immer ein weiteres Abrechnungsinstitut mit einbezogen, was in der Regel bedeutet, daß das Gutschreiben von Finanzmitteln verzögert stattfindet. Zur Überprüfung der Liquidität eines Kunden muß eine meist recht kostenintensive Verbindung zu einem Bankenrechenzentrum hergestellt werden oder bestehen. Bargeld hat den Vorteil, daß es nur auf Echtheit überprüft werden muß, ansonsten aber automatisch für die Liquidität des Kunden steht.

Vermehrt wird der Wunsch geäußert, neue Zahlungsmittel einzuführen, die es ermöglichen, Bezahlungsvorgänge anonym durchzuführen. Schlagworte wie „Käuferprofil“ und zielgerichtete Werbung sind in diesem Zusammenhang zu nennen. Gefordert werden Zahlungsmittel, die von ihrer Struktur dem Bargeld entsprechen, d.h.

– sie müssen einfach und schnell einsetzbar sein,

– sie stellen an sich einen Wert (ähnlich einem Geldschein) dar,

– sie müssen deshalb eigene Echtheitsmerkmale besitzen,

– sie müssen in verschiedenen Stückelungen, auch als Kleinstbeträge vorliegen.

Der letzte Punkt ist gerade für das Bezahlen von Inhalten des Internet interessant (z.B. die Genehmigung, bestimmte Webseiten anzusehen), da es hier meist um Pfennigbeträge geht, bei denen eine Abrechnung jeder Transaktion über eine Bank oder ein Kreditkarteninstitut zu umständlich wäre.

Cybermoney – das neue digitale Geld

Die auf dieser Grundlage entwickelten Systeme lassen sich unter dem Oberbegriff „Cybermoney“ zusammenfassen. Hierunter versteht man grundsätzlich jegliche Art digitalen oder elektronischen Geldes (also auch z.B. den Betrag der neuerdings auf einer EC-Karte/Geldkarte gespeichert werden kann). Im engeren Sinne ist hiermit jedoch Netzgeld gemeint, also ein Zahlungsmedium, mit dem in Computernetzen, wie dem Internet, bezahlt werden kann.

Bei den auf elektronischem Wege geschaffenen Werteinheiten (auch: „Cyberbucks“ oder „Cyberbills“) handelt es sich um völlig eigenständige, „künstliche“ Währungen, die eine weltweite Bezahlung von Waren und Dienstleistungen über das Internet ermöglichen.

Die Deutsche Bank führt seit Herbst 1997 einen Versuch mit 1500 Kunden durch. Dafür wird das System der niederländischen Firma DigiCash, ecash, eingesetzt. Erklärtes Ziel des Initiators dieses Systems, David Chaum, ist die absolute Anonymität des Zahlungsverkehrs.Um dies umzusetzen, wird folgendes Verfahren angewandt:

Der Kunde erstellt auf seinem Rechner Werteinheiten und überspielt sie an seine Bank. Die Bank verrechnet den entsprechenden Betrag mit dem Kundenkonto und „druckt“ ein „Echtheitszertifikat“ auf. Dabei bekommen die Werteinheiten keine Zuordnung zu einem bestimmten Kunden „aufgedruckt“, sondern nur ein allgemeines Echtheitszertifikat. Die Bank nimmt diese Werteinheiten später von anderen Kunden zurück und schreibt sie deren Konten gut.

Der Kunde kann nun seinerseits die Werteinheiten im Internet bei Anbietern, die sich diesem System angeschlossen haben, wie Bargeld benutzen. Er übergibt eine Datei genau an der Stelle des Kaufvorgangs, an der er früher seinen Geldbeutel gezückt und einen Geldschein übergeben hätte. Die Anbieter verrechnen die Werteinheit in der ersten Phase des Projektes wieder mit der ausgebenden Bank, wobei nicht nachzuvollziehen ist, von wem die Werteinheiten ursprünglich stammen. Ein Verfahren ähnlich dem Bargeldverkehr.

Bisher soll nach Aussage der Deutschen Bank dieses Verfahren nur zur Begleichung von Kleinstbeträgen (bis maximal 400 DM) zum Einsatz kommen. Es soll also gerade zur Bezahlung von Dienstleistungen benutzt werden.

Es werden Systeme erprobt, Cybermoney durch eine elektronische Übertragung von Werteinheiten, die auf dem Geldchip der EC-Karte gespeichert werden, zu realisieren. Es geht darum, Werteinheiten vom Kunden zum Händler oder von der Bank zum Kunden zu übertragen.

Da das Internet nach Einschätzung von Fachleuten in den nächsten Jahren verstärkt zum Handelsmedium ausgebaut werden soll (die Bundesregierung

geht von einem möglichen Handelsvolumen von 500 Milliarden Mark weltweit im Jahr 2001 aus), ist es gut vorstellbar, daß es spätestens dann möglich werden wird, größere Summen per Cybermoney zu transferieren. Es entsteht ein System, das für die Banken eine wesentliche Arbeitsvereinfachung durch Automatisierung mit sich bringt, dadurch einen Bruchteil der Kosten verursacht und weniger Personal als das herkömmliche Filialnetz benötigt.

Weitere Effekte, die bei der Verbreitung von Cybermoney zu erwarten sind:

– die Währungshoheit der Nationalbanken wird untergraben, da immer mehr Privatinstitute als Herausgeber einer Währung in Erscheinung treten. Hierbei kommt es lediglich darauf an, daß der Kunde Vertrauen in den Herausgeber der Währung hat, da dieser in gewissem Maße für die Wertstabilität Verantwortung trägt;

– die Anzahl der Währungen wird in einem ersten Schritt größer und unübersichtlicher (die Dresdener Bank hat sich für ein anderes System als die Deutsche Bank entschieden);

– die Besteuerung von Waren, Dienstleistungen und Arbeit wird problematischer. So kann z.B. ein Computerprogrammierer seine in Deutschland erstellte Software über das Internet in ein beliebiges Land übertragen und dafür Cybermoney als Bezahlung erhalten. Dieses Geld kann dann wieder zum Kauf von Waren oder Dienstleistungen eingesetzt werden. An welcher Stelle die deutschen Finanzbehörden noch auf die Transaktionen aufmerksam werden und entsprechende Steuern einfordern können, ist noch nicht geklärt;

– eine mögliche Fälschung von Geld oder andere Gründe, warum die Entwertung einer Sorte Cybermoney stattfinden kann (z.B. Konkurs der Herausgeberfirma, Fehler in der Buchungssoftware etc.), hätten Folgen, die man bisher nur erahnen kann.

Es ist also wichtig, auf einen größtmöglichen Fälschungsschutz und Buchungssicherheit hinzuwirken. Ob sich die notwendige internationale „Bankenaufsicht" über die Firmen und Geschäftsbanken, die in Zukunft als Notenbank auftreten, realisieren läßt, bleibt abzuwarten.

Das für die Polizei wichtigste Problem dürften die neuen Möglichkeiten zur Geldwäsche sein.

Während der Straftäter heute noch das Bargeld von Land zu Land transportieren muß und sich dabei dem Risiko des Verlustes oder der Kontrolle ausgesetzt sieht, können in Zukunft weltweite Finanztransaktionen vom heimischen PC in einfacher Weise und anonymisiert vorgenommen werden.

Hier muß darauf hingewirkt werden, daß Transaktionen nachvollziehbar bleiben, auch wenn andere Interessen dem entgegen stehen. Andernfalls müssen Ermittlungsstrategien im Bereich Geldwäsche grundsätzlich neu überdacht werden.

Ermittlung und Beweissicherung im Internet

Eine notwendige technische Ausstattung für Dienststellen, die mit Ermittlungen bzw. der Beweissicherung im Internet betraut sind, könnte folgendermaßen aussehen:

– PC als Einzelplatz-PC, d.h. ohne Verbindung zu sensiblen dienstlichen Daten, (kann auch dadurch realisiert werden, daß ein vorhandener PC mit einem Wechselfestplattensystem ausgerüstet wird, um die Anschaffung eines zusätzlichen Computers zu vermeiden),

– Internet-Zugang über ISDN-Karte oder Modem,

– Internet-Zugang bei einem Provider, der über eine ausreichende Bandbreite für eine schnelle Datenübertragung verfügt,

– weitere Internet-Zugänge, um Zugang zu mehreren Newsservern und anderen Netzinhalte zu erhalten, die durch einzelne Provider nicht angeboten werden,

– verdeckte Internet-Zugänge für Ermittlungsmaßnahmen in diesem Bereich,

– Zugangssoftware und Tools für alle Dienste des Internet,

- Hilfsmittel für die Beweissicherung und -dokumentation: (Farb-) Drucker, Datenspeicher.

Inwieweit zentrale Einrichtungen für die gesamte deutsche Polizei, so z.B. ein zentraler Newsserver oder ein polizeieigener Provider sinnvoll sind, ist zu prüfen.

Die für diese Aufgaben zuständigen Sachbearbeiter müßten sich laufend fortbilden, um mit der rasanten technischen Entwicklung Stand zu halten.

Aufgrund der Flüchtigkeit der Inhalte des Internet muß immer unverzüglich mit der Beweissicherung begonnen werden.

Angriffe auf Daten durch das Internet

Dadurch, daß ein Computer mit dem Internet verbunden wird, bestehen verschiedene Möglichkeiten, auf seine Daten zuzugreifen. Aus diesem Grund sollten keine sensiblen Daten auf einem Rechner vorhanden sein, der mit dem Internet verbunden ist. Bei der Verbindung von Firmennetzwerken mit dem Internet sollte eine sogenannte „Firewall" zum Einsatz kommen. Diese besteht aus einem zentralen Rechner, über den alle Verbindungen zum Internet realisiert werden. Auf diesen Rechner wird eine Software instal-

liert, die nur bestimmte Daten durchläßt und so den Zugriff von außen beschränken soll. Die „Firewall" muß ständig an neue Angriffsmethoden angepaßt werden.

Nach einem erfolgten Angriff ist es unter Umständen möglich, über Protokolle die Spur zu verfolgen. Solche Protokolle sollten überall dort Verwendung finden und gewissenhaft geführt werden, wo Computernetzwerke zum Einsatz kommen.

Eine besondere Gefährdung geht von den Technologien aus, die es ermöglichen, ausführbare Programme (sogenannte Applets) bei Bedarf aus dem Internet zu laden, und dann direkt auf einem Computer ablaufen zu lassen.

Bei der Benutzung dieser Technologie sollten alle Sicherungsmöglichkeiten genutzt werden, da sonst ungewollte und schädliche Programmabläufe gestartet werden können.

Neben der Programmiersprache JAVA ist hier insbesondere die ActiveX-Technologie von Microsoft zu nennen. Diese ist gerade darauf ausgerichtet, vom Benutzer nicht mehr zu kontrollierende Abläufe auf einem Computer zu starten. So wurde z.B. durch Mitglieder des Chaos Computer Club demonstriert, wie solch ein Angriff aussehen könnte. Während einer Internet-Sitzung wurde durch Zugriff auf eine bestimmte WWW-Seite und durch Anklicken eines Button unbemerkt im Hintergrund ein ActiveX Applet gestartet. Dies bewirkte, daß auf dem Rechner eine Banküberweisung ausgefüllt wurde, die dann bei der nächsten Übermittlung von Überweisungen an eine Bank unbemerkt im Hintergrund mit übertragen worden wäre. Ob eine Absicherung vor solchen Angriffen bei der Benutzung von ActiveX möglich ist, wird wiederholt in Zweifel gezogen.

Eine weitere Angriffsmöglichkeit entsteht dann, wenn Daten über das Internet übertragen werden. Da die Datenübertragung im Internet grundsätzlich offen ist, sollten sensible Daten vor der Übertragung sinnvoll verschlüsselt werden, wobei hierdurch wieder Probleme in den Fällen entstehen, in denen auf diese Daten im Ermittlungsverfahren zugegriffen werden muß. Hier ist noch kein Weg gefunden, der alle Faktoren berücksichtigt.

Auch Mord ist möglich

Aufgrund des zunehmenden Einsatzes der Computertechnik in Krankenhäusern und bei Ärzten kann der perfekte Mord, die sogenannte „Online-Tötung" begangen werden. Bereits heute wird die Medikamentierung für einzelne Patienten in einem Computer festgehalten. Die zuständige Schwester stellt dort die verschriebene Menge fest und verabreicht das Medikament entsprechend. Sollte der Zugriff auf solch einen Rechner von außen möglich sein, könnte der Mörder die Medikamentenmenge verändern, so daß daraus eine tödliche Dosis entsteht. Später könnte er dann die ursprüngliche Angabe wieder herstellen. Jegliche Spur wäre verwischt.

Internationaler Aspekt erschwert Ermittlungen

Die internationale Ausdehnung des Internet kann Ermittlungen gehörig erschweren:

– Daten können in jedem beliebigen Land der Erde abgespeichert werden,

– Daten können beliebig verteilt oder gespiegelt (kopiert) werden, auch sonst kann im Rahmen von bestimmten Aktionen gezielt ins Ausland ausgewichen werden,

– in den unterschiedlichen Ländern herrschen voneinander abweichende Rechtsvorstellungen,

– bestimmte Länder sind generell nicht zur Zusammenarbeit bereit,

– weltweite Verbindungen und Transaktionen sind in Sekundenschnelle möglich,

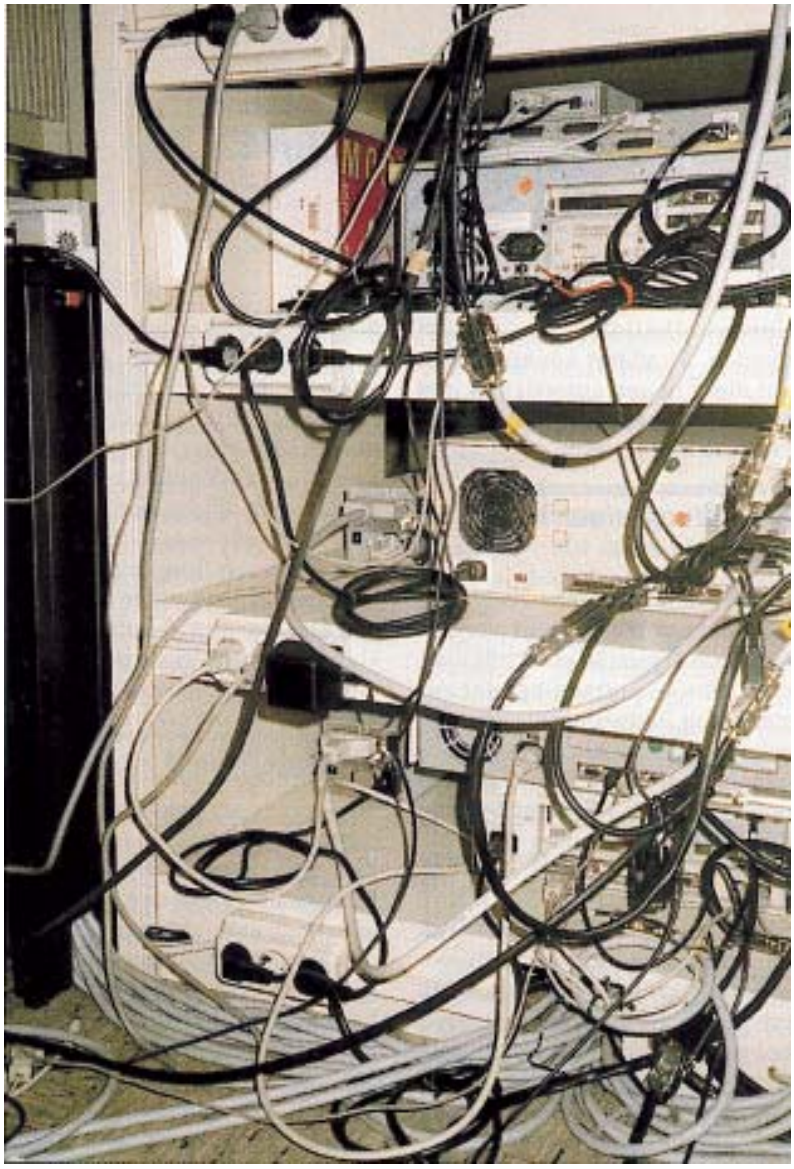
– es sind im elektronischen Netz keine Grenzen vorhanden.

Deshalb macht es Sinn internationale Regelungen anzustreben.

Aus dem Teledienstgesetz (TDG) ist keine Vorschrift ersichtlich, nach der Dienstanbieter verpflichtet sind, Kundendaten auf Anforderung an Strafverfolgungsbehörden weiterzugeben. Nach § 89 (6) Telekommunikationsgesetz (TKG) sind Anbieter, die geschäftsmäßig Telekommunikationsdienste erbringen, verpflichtet, personenbezogene Daten, im Einzelfall auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten oder zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung erforderlich ist.

Der Wirkungsbereich des TKG ist im Bezug auf die Internet-Provider nicht eindeutig geregelt. So treten Probleme bei den Definitionen im § 3 TKG und dadurch bei den Auskunftsregelungen nach § 90 TKG auf. Eine eindeutige Regelung und Nennung wäre wünschenswert.

Anders als im Bereich der Mobilfunk- oder Festnetzbetreiber besteht im Bereich der Internet-Provider kein gesetzliches Zulassungsverfahren. Dies bedeutet einerseits, daß jedermann Provider werden kann und andererseits keine Liste besteht, in der alle in Deutschland tätigen Provider aufgeführt sind. In der Praxis wirkt sich dies so aus, daß beim polizeilichen Anfragen an Provider gemäß § 89 TKG nicht sichergestellt ist, daß der Vorgang beim Provider entsprechend vertraulich und sachgemäß behandelt wird. Außerdem ist es schwierig, die Gesamtheit alle Provider



Geheimnisvolle Ordnung im Gewirr der Kabel. Foto: -lt

anzusprechen, wenn z.B. im Sinne des § 5 (2) TDG die Provider auf kriminelle Inhalte des Internet hingewiesen werden sollen, um sie zu einer Sperrung zu veranlassen.

Für diesen Bereich wäre es sinnvoll, geeignete Lizenzierungsverfahren zu schaffen bzw. die Provider in einer anderen, geeigneten Weise zu erfassen. Auf jeden Fall gilt es, beim Umgang mit Providern eine erhöhte Wachsamkeit an den Tag zu legen. Aus den genannten Gründen wäre es sinnvoll, die Provider in ein automatisiertes Verfahren nach § 90 TKG aufzunehmen.

Ermittlung von Email-Adressen

Der Verantwortliche für einen Mailserver sowie für jeden anderern Rechner im Internet ist einfach zu ermitteln. Da die Namensvergabe für jedes Land zentral geregelt und registriert wird, kann über eine Online-Anfrage im WWW bei der entsprechenden Zentrale (für Deutschland z.B. unter http://www.nic.de; „Whois“ Abfrage) die verantwortliche Person für eine Internetadresse, bestimmt werden.

Bei den Email-Servern, die von Providern betrieben werden, kann dann, da diese in der Regel im Inland betrieben werden, der Besitzer einer Email-Adresse namentlich ermittelt werden. Dieser ist für das notwendige Abrechnungsverfahren beim Provider bekannt. Maßnahmen der Postbeschlagnahme oder -überwachung können bei diesem Provider eingeleitet werden, wobei diese Funktionen teils unter großem Kostenaufwand für einen Mailserver programmiert werden muß. Außerdem ist die Vertraulichkeit des Providers sicherzustellen. Wesentlich problematischer sind die Fälle, in denen eine Email-Adresse über das WWW abgefragt wird. Der dazugehörige Mailserver kann an einem beliebigen Ort auf der Welt stehen. Somit ist das Herantreten an den Betreiber mit vielfältigen Problemen (Rechtshilfe, Zeitverzug) verbunden oder gar unmöglich.

Ein weiteres Problem ist auch, daß zum Benutzen einer solchen Adresse meist keine eindeutige Personalienangabe des Nutzers nötig ist, da dieser Dienst für ihn kostenfrei angeboten wird. (Die Betreiber finanzieren sich über in die Postfächer eingeworfene Werbung, wollen ihre technischen Fähigkeiten demonstrieren oder gezielt eine Möglichkeit für den anonymisierten Email-Verkehr schaffen.)

In solchen Fällen ist dann nur über technische Protokolle nachvollziehbar, welcher Nutzer das entsprechende Email-Postfach betreibt, was entweder mit einem hohen technischen Aufwand verbunden oder ganz unmöglich ist.

Die Sicherstellung von Email-Nachrichten ist rechtlich nicht problematisch. Allerdings sind die technischen Verfahren noch nicht bei allen Providern vorhanden, so daß auch hier eine gesetzliche Vorschrift, beziehungsweise eine Erweiterung der Gültigkeit des § 88 TKG für Internet-Provider sinnvoll wäre. Auch ist zu prüfen, ob und inwieweit die Überwachung anderer Kommunikationsmöglichkeiten, die durch das Internet angeboten werden (z.B. Internet-Telefonie), gesetzlich geregelt und technisch möglich gemacht werden sollte, da hier herkömmliche

Kommunikationswege ersetzt werden. Straftäter könnten sonst auf diese neuen ausweichen und Maßnahmen nach § 100a StPO ins Leere laufen lassen.

Ermittlung einer Web-Adresse

Der Standort eines Anbieter-Rechners und die dafür verantwortliche Person ist ebenfalls über eine Who-is-Anfrage bei der zuständigen Registrierungszentrale erfragbar. Probleme gibt es bei Inhalten, für die in anderen Ländern unterschiedliche Einschätzungen der Strafbarkeit gelten. Dies gilt insbesondere für den Bereich Staatsschutzkriminalität und Kinderpornographie. In der Regel wird der Hinweis über international strafrechtlich relevante Web-Inhalte an die zuständige Polizeibehörde eines Landes weitergeben. Im Inland wird direkt gegen den entsprechenden Betreiber des Rechners, bzw. den Anbieter der entsprechenden Inhalte ermittelt.

Probleme treten dann auf, wenn die Netzgemeinschaft den Inhalt unter dem Gesichtspunkt der freien Meinungsäußerung erhalten will, und ihn durch Spiegelung auf eine Vielzahl von Rechnern verbreitet. Ob der Empfang von einzelnen Inhalten durch bestimmte deutsche Provider technisch zu sperren ist, ist umstritten. Der Sperrung steht auf alle Fälle der oben beschriebene Vorgang der Spieglung von Inhalten auf andere Rechner entgegen. Außerdem ist zu bedenken, daß keine Gesamtliste der deutschen Provider besteht, so daß Sperrungsverfügungen nur an die zugestellt werden können, die der zuständigen Behörde bekannt sind.

Ermittlung von Newsgroups

Bei der Verbreitung von strafrechtlich relevanten Inhalten in Newsgroups ist möglichst der ursprüngliche Einsteller einer bestimmten Nachricht zu ermitteln. Dieser hinterläßt im Normalfall eine Email-Adresse als Möglichkeit für eine Kontaktaufnahme. Dann treten die Probleme auf, die bereits beschrieben wurden. Aus den technischen Protokollen (Header), die zu jeder Nachricht erstellt werden, können unter Umständen Hinweise erzielt werden, von welchem Rechner aus die Nachricht in die Newsgroup eingestellt wurde.

Sperrungen einer bestimmten Newsgroup sind meist nicht weitreichend genug. Es existieren neben den von dem jeweiligen Provider betriebenen Newsservern noch eine Vielzahl von sogenannten Public-News-Servern, die von jedem Teilnehmer des Internet benutzt werden können und eine Vielzahl von Newsgroups anbieten.

Ein problematischer Bereich für die Polizei sind Anzeigen, die den Inhalt von Newsgroups betreffen. Zum einen können die Nachrichten bereits gelöscht sein, da die polizeiliche Bearbeitungsdauer eines solchen Vorgangs länger dauern kann, als die Frist, innerhalb derer eine Nachricht gespeichert bleibt. Ein weiteres Problem besteht darin, daß die beweissichernde Dienststelle keinen Zugang zu der angezeigten Newsgroup hat. Gerade im Bereich Kinderpornographie werden von vielen deutschen Providern bestimmte Newsgroups nicht angeboten. Zur Beweissicherung ist dann eine umfangreiche Suche auf den Public-News-Servern notwendig. Hier wäre die Einrichtung eines polizeieigenen Newsservers zu prüfen. Für diesen könnten dann alle benötigten Newsgroups aus dem Internet abonniert werden. Daten könnten über einen längeren Zeitraum gespeichert bleiben, und damit spätere Ermittlungen möglich machen.

Online-Durchsuchung

Eine weitere Problematik, die durch den Einsatz von Computernetzwerken auftritt, ist die Möglichkeit, Daten auf einem entfernt stehenden Rechner (teilweise sogar im Ausland) zu lagern, und trotzdem über eine Datenleitung jederzeit auf diese Daten zuzugreifen. Damit können Probleme im Rahmen von Ermittlungsmaßnahmen entstehen, so z.B. bei der Datensichtung im Internet oder bei Durchsuchungsmaßnahmen, bei denen festgestellt wird, daß eine Verbindung zu einem entfernt stehenden Rechner besteht.

Beim polizeilichen Zugriff auf Daten, die nicht durch Paßwortsysteme o.ä. besonders gesichert sind, liegt kein Eingriff in Grundrechte vor. Beim Vorhandensein solcher Sicherungssyteme sollte eine Ermächtigungsgrundlage vorliegen. Der § 100 a StPO stellt hier keine eindeutige Rechtsgrundlage dar, da es nicht um die Überwachung einer Kommunikation zwischen zwei Parteien, sondern um den Zugriff durch die Polizei auf vorhandene Datenspeicher einer anderen Person oder Institution geht. Hierzu äußerte sich die Arbeitsgruppe PCPC des Europarats:

„1. Die gesetzlichen Unterschiede zwischen der Durchsuchung automatisch verarbeiteter und der Überwachung und Aufzeichnung automatisch übertragener Daten sollten genau beschrieben und beachtet werden.

2. Das Strafprozeßrecht sollte es den Ermittlungsbehörden erlauben, Computersysteme unter ähnlichen Bedingungen wie bei traditionellen Durchsuchungs- und Beschlagnahmebefugnissen zu durchsuchen und Daten zu beschlagnahmen. Zusätzlich sollte die für das System verantwortliche Person darüber informiert werden, daß das System durchsucht wurde und welche Arten

von Daten beschlagnahmt wurden. Die allgemein gegen Durchsuchungen und Beschlagnahmen vorgesehenen Rechtsbehelfe sollten im Falle der Durchsuchung und der Beschlagnahme der darin enthaltenen Daten in gleicher Weise anwendbar sein."

Unter der Durchsuchung von Computersystemen sind auch paßwortgeschützte Anbieterrechner im Internet zu verstehen. Ein zusätzliches Problem entsteht, wenn der datenspeichernde Rechner im Ausland steht, da der Zugriff dann den Vorschriften der internationalen Rechtshilfe unterliegt. Für diesen Bereich lautet der Empfehlungsentwurf der Arbeitsgruppe PCPC:

„13. Die Befugnis, eine Durchsuchung auf andere Computersysteme auszuweiten, sollte, sofern sofortiges Handeln erforderlich ist, auch bestehen, wenn ein Computersystem einer ausländischen Gerichtsbarkeit untersteht. Um mögliche Verletzungen der staatlichen Souveränität oder des Völkerrechts zu vermeiden, sollte eine unzweideutige Grundlage für derartige Durchsuchungen oder Beschlagnahmen geschaffen werden. Daher sollten internationale Vereinbarungen ausgehandelt werden, die regeln, wie, wann und in welchem Umfang derartige Durchsuchungen und Beschlagnahmen erlaubt sein sollen.

14. Soweit gesetzlich noch nicht vorgesehen, sollte in Erwägung gezogen werden, für Fälle, in denen unverzügliches Handeln erforderlich ist, beschleunigte Verfahren zu schaffen, die es den Ermittlungsbehörden erlauben, in einem Computersystem enthaltene Daten auf Ersuchen ausländischer Ermittlungsbehörden zum Zwecke ihrer Übermittlung gemäß den einschlägigen Bestimmungen über die gegenseitige Rechtshilfe unverzüglich zu beschlagnahmen.

Auf ähnliche Weise sollte auch die Schaffung beschleunigter Verfahren sowie eines Verbindungssystems in Erwägung gezogen werden, damit Übermittlungsdaten hinsichtlich einer bestimmten Datenübertragung unverzüglich zur Verfügung gestellt, eine bestimmte Datenübermittlung überwacht und aufgezeichnet oder ihr Ausgangspunkt ermittelt werden kann."

Dem ist nichts hinzuzufügen.

Verdeckte Ermittlungen

Ermittlungen im Internet können in einzelnen Fällen nur verdeckt durchgeführt werden, um Aussicht auf Erfolg zu haben. Hierfür bedarf es einer speziellen Eingriffsnorm. Sofern auf uneingeschränkt offen zugängliche Daten aus öffentlichen Datennetzen zugegriffen wird, handelt es sich um schlicht hoheitliches Handeln auf Grundlage der gesetzlichen Aufgabenzuweisung, das keiner weiteren speziellen Befugnis bedarf. Für Zugriff auf Daten, die speziell gesichert sind und dadurch nur für einen bestimmten Kreis von Personen zugänglich sind, ist eine Befugnisnorm notwendig.

Für entsprechende präventivpolizeiliche Maßnahmen enthalten die Polizeigesetze der Länder die erforderlichen Befugnisnormen. Auf dieser Grundlage sind einzelne, gefahrenabwehrende, verdeckte, zeitlich befristete Datenerhebungen, die ohne wesentlichen organisatorischen, personellen und technischen Aufwand durchgeführt werden, zulässig.

Dies gilt auch für Maßnahmen im strafprozeßualen Bereich. Der hier ermittelnde Beamte handelt als Nicht offen ermittelnder Beamter (NoeP), dessen Befugnisse sich nach den allgemeinen Bestimmungen der StPO richten.

In den Fällen, in denen

– nur durch besonderen technischen Aufwand Daten eingesehen werden können (Hard oder Software; z.B. zur Überwindung von Zugangs/Zugriffssperren),

– besonderer organisatorischer Aufwand erforderlich ist, zum Beispiel einer auf Dauer angelegte Legende des / der Ermittlungsbeamten,

ist eine weitergehende Eingriffsnorm notwendig. Diese ist durch § 110a StPO und die entsprechenden Befugnisnormen der Polizeigesetze der Länder gegeben. Ihre Anwendbarkeit ist in jedem Einzelfall zu prüfen.

Anlaßunabhängige Ermittlungen

Daß die Polizei auf Hinweis und Anzeigen reagieren muß, die Inhalte des Internet betreffen, ist unstrittig. In diesen Fällen wird die Strafbarkeit von Inhalten festgestellt, Beweise gesichert, Verantwortliche ermittelt und entsprechende weitere Maßnahmen eingeleitet. In der Mehrzahl der Fälle bedeutet dies, daß auf dem polizeilichen Dienstweg ausländische Dienststellen über strafrechtlich relevante Sachverhalte informiert werden, die von ihrem Land aus im Internet angeboten werden.

Einen besonderen Bereich der polizeilichen Arbeit stellen die sogenannten anlaßunabhängigen Ermittlungen im Internet dar. Hier geht es darum, daß die Polizei im Internet ermittelt, ohne daß ein konkreter Tatverdacht gemäß § 152 StPO vorliegt. Es liegen allerdings Anhaltspunkte vor, die dafür sprechen, daß strafbare Inhalte im Internet verbreitet werden.

Rechtsgrundlage für solche Initativermittlungen sind die Polizeigesetze der Länder. Aufgrund der riesigen Datenmenge des Internet sind Initativermittlungen äußerst personal- und zeitintensiv. Da das Internet nicht ein

örtlich gebundenes, sondern ein weltweit benutzbares Medium ist, sind von vielen Orten aus dieselben Feststellungen zu machen. Es ist deshalb nicht sinnvoll, an vielen Stellen unkoordiniert solche anlaßunabhängigen Ermittlungen zu führen, sondern sie zu bündeln.

Anlaßbezogene Informationsgewinnung

Ein nicht zu vernachlässigender Aspekt des Internet ist die Fülle von Informationen, die auch dazu genutzt werden können, die polizeiliche Arbeit zu unterstützen. So kann z.B. Aufklärung zu polizeilichen Großlagen (Chaostage, Castortransport etc.) betrieben werden, oder es kann die tägliche polizeiliche Arbeit durch Informationen zu bestimmten Themen begleitet werden. Hier hat es sich als sinnvoll erwiesen, den fachlich zuständigen Beamten durch dafür sachkundige Beamte zu unterstützen, um die Suche im Internet möglichst zielgerichtet und zeitsparend durchzuführen.

Meldedienst

Dadurch, daß das Internet nicht auf einen Ort fixiert ist, besteht die Gefahr von Mehrfach-Ermittlungen in einem Sachverhalt. Deshalb ist es sinnvoll, Daten zentral zu sammeln, damit ein bundesweites Lagebild erstellt werden kann. Auch wird dadurch die Täter- bzw. Tatzusammenführung möglich.

Zu diesem Zweck wurde der Meldedienst I.u.K. (Informations- und Kommunikations-) Kriminalität von der AG Kripo eingeführt. Dadurch sind alle Fälle der Kriminalität im Zusammenhang mit dem Internet meldepflichtig. Dieser Meldedienst ist aber nicht nur auf diesen Bereich beschränkt, sondern betrifft eine Vielzahl von weiteren Delikten (z.B. den Einsatz von Telefonkartensimulatoren oder die Softwarepiraterie).

Verantwortlichkeit der Provider

Inwieweit Provider für Daten verantwortlich sind, die von ihnen zu ihren Kunden übertragen werden, war in der Vergangenheit umstritten. Die Anklage gegen Ex-Compusserve-Geschäftsführer Felix Somm wegen Verbreitung pornographischer und gewaltverherrlichender Schriften hat die Problematik deutlich gemacht. Mit der Verabschiedung des Teledienstegesetz (TDG) wurde im § 5 eine gesetzliche Grundlage für die Verantwortlichkeit der Provider geschaffen:

(1) Diensteanbieter sind für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von den Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern.

(3) Diensteanbieter sind für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht verantwortlich. Eine automatische und kurzzeitige Vorhaltung fremder Inhalte auf Grund Nutzerabfrage gilt als Zugangsvermittlung.

(4) Verpflichtungen zur Sperrung der Nutzung rechtswidriger Inhalte nach den allgemeinen Gesetzen bleiben unberührt, wenn der Diensteanbieter unter Wahrung des Fernmeldegeheimnisses gemäß § 85 des Telekommunikationsgesetzes von diesen Inhalten Kenntnis erlangt und eine Sperrung technisch möglich und zumutbar ist.

Hilfsmittel Perkeo

Eine Kontrolle von Internet-Inhalten, insbesondere der Newsgroups, ist bei den vorhandenen riesigen Datenmengen nur in einem automatisierten Verfahren zu realsieren. Eine Durchsicht von Newsgroups „per Hand" wäre auch beim Einsatz einer Vielzahl von Personen nicht möglich.

Das Problem bestand bisher darin, automatisierte Verfahren so einzurichten, daß sie mit einer geringen Fehlerquote die in Frage stehenden Inhalte erkennen. So wurde z.B. durch Scansoftware auf der Suche nach Darstellungen von nackten Personen das Bild eines Leuchtturms als Treffer markiert. Häufig soll auch nicht nach jeglichen pornographischen Darstellungen gesucht werden, sondern explizit nach kinder- oder tierpornographischen.

Zum diesem Zweck wurde durch einen Mitarbeiter des LKA Hessen die Software „Perkeo" (Programm zur Erkennung relevanter kinderpornographischer eindeutiger Objekte) entwickelt. Für diese Software wird zu allen bekannten Bildern mit Kinder- oder Tierpornographie ein elektronischer Fingerabdruck erstellt. Dieser benötigt wesentlich weniger Speicherplatz als das Originalbild, so daß hieraus eine nicht zu große Datenbank erstellt werden kann. Diese Datenbank wird ständig durch neue Abbildungen ergänzt. Perkeo wurde als Hilfsmittel für die Sichtung von Computern während einer laufenden Durchsuchung entwickelt. Es ist aber auch einsetzbar, um Internet-Inhalte, insbesondere in Newsgroups, zu überprüfen.

Perkeo vergleicht die auf einem Rechner oder in einer Newsgroup vorhandenen Bilddateien mit denen der Datenbank und zeigt eventuell vorhandene Treffer an. Somit kann vor Ort über die Sicherstellung eines Computers ent-

schieden werden. Erkannte Beiträge können aus einer auf einem Server geführten Newsgroup gelöscht werden.

In wieweit diese Software eine technische Möglichkeit darstellt, die es für Diensteanbieter zumutbar macht, die Nutzung von fremden Inhalten zu verhindern, wie im § 5 (2) TDG gefordert wird, ist noch zu klären. Provider könnten also in Zukunft verpflichtet werden, diese oder andere Scansoftware auf den von ihnen betriebenen Newsservern einzusetzen. Weitere Einsatzmöglichkeit für die Software, z.B. um nach jugendschutzrelevanten Inhalten zu suchen oder bei der Auswertung von Datenträgern zu helfen, werden momentan entwickelt.

Freiwillige Selbstkontrolle auch im Internet möglich

Internet-Inhalte die von einer längerfristigen Natur sind, z.B. WWW-Seiten, bieten die Möglichkeit, „per Hand" gesichtet zu werden. So werden z.B. Systeme erprobt, bei denen der Ersteller einer Seite im Wege der freiwilligen Selbstkontrolle die Möglichkeit hat, diese erst ab einer bestimmten Altersgruppe freizugeben. Diesen Vorgang nennt man Rating. Es werden auch weitere Personen für die Klassifizierung mit einbezogen. Auf der Seite des Anwenders werden dann entsprechende Programme installiert, die nur den Zugang zu den so klassifizierten Seiten anbieten. Es ist dann z.B. möglich, für jedes Familienmitglied einem dem Alter entsprechenden Internet-Zugang zu realisieren.

Diese Systeme sind davon abhängig, ob sie vom Nutzer angenommen werden. Sie sind sicher ein Weg, jugendgefährdende Inhalte von der entsprechenden Zielgruppe fernzuhalten.

Folgende Punkte sind jedoch als problematisch anzusehen und sollten noch gelöst werden, damit ein sinnvolles System entsteht:

– Es besteht die Möglichkeit, entsprechende Sperrungen am Computer zu umgehen. Hier hat es sich gezeigt, daß gerade Kinder und Jugendliche in der Ausnutzung und dem Gebrauch der Technik ihren Eltern überlegen sind;

– dem Nutzer wird nur ein bestimmter Bereich des Internet präsentiert, nämlich der, der bereits klassifiziert ist. Dies ist durch die riesigen Datenmengen des Internet als schwierig anzusehen. Außerdem konkurrieren zur Zeit noch mehrere Systeme miteinander, so daß kein einheitlicher Standard besteht. Anbieter eines Inhaltes müssen diesen also für mehrere Systeme klassifizieren, um für jeden Anwender erreichbar zu sein;

– die Realisierung der oben beschriebenen Möglichkeiten, die Verbreitung von straftrechtlich und jugendschutzrelevanten Inhalten des Internet zu erschweren, muß geprüft werden. Nach wie vor bleibt die Aufgabe der Polizei, die Urheber dieser Inhalte des Internet zu ermitteln, bestehen.

Steganografie – Daten verstecken

Als Ergänzung zu den weitverbreiteten Verschlüsselungssystemen, die im Internet Verwendung finden, ist die sogenannte Steganografie zu sehen. Hier geht es darum, Daten, teilweise als Ergänzung zur Verschlüsselung, zu verstecken. Dieser Grundgedanke ist bereits 2000 Jahre alt. So wurden im alten Griechenland Nachrichten auf die Kopfhaut eines Boten tätowiert. Getarnt durch die nachgewachsenen Haare konnten dann geheime Nachrichten durch die Linien des Feindes getragen werden.

Heutzutage werden Texte oder sonstige Daten in anderen Dateien versteckt. Hierzu finden vor allem Bilder und Tondateien Verwendung. Die zu versteckenden Daten werden mit Hilfe eines Softwareprogramms in den Programmcode der „Wirtsdatei" eingefügt. Hierdurch wird z.B. bei einer Bilddatei maximal eine Farbveränderung am Bild und/oder eine Veränderung der Dateigröße bewirkt. Es ist bei einer Vielzahl von Bildern, die heutzutage auf vielen Rechnern gespeichert sind, kaum zu erkennen, welche Datei als Versteck gebraucht wurde. Zum Herausholen der versteckten Daten benötigt man dieselbe Software, die zum Verstecken genutzt wurde.

Polizei muß Schritt halten

Einerseits entsteht durch das Internet eine ganz neue Form von Kriminalität, die ohne Internet nicht möglich war. Andererseits bietet das Internet ungeahnte Möglichkeiten, klassische Straftaten mit modernen Mitteln zu begünstigen. Die technische Fortentwicklung und die zunehmende Bedeutung des Internet sind Anlaß genug dafür, dieses Kommunikations- und Interaktionsmittel ständig im Auge zu behalten. Es bleibt der Polizei nichts anderes übrig, als Schritt zu halten, um nicht von neuen Bereichen der Kriminalität abgehängt zu werden.