International Conference
on IT-Incident Management & IT-Forensics

IT based crime: Evidence Collection & Legal Restrictions in Investigation Cases

Computer-unterstützte Kriminalität: Aufklärung und Tatnachweis am Beispiel sogenannter Phishing-Verfahren

Oberstaatsanwalt Jens Gruhl, Konstanz

Stuttgart, September 12, 2007

1 Computerkriminalität

Computerkriminalität ist nichts neues. Die Polizeiliche Kriminalstatistik vergangener Jahre hat immer wieder Höchstwerte der Computerkriminalität ausgewiesen. Dabei handelte es sich aber vorrangig um die missbräuchliche Verwendung von Eurocheque-Karten - ein klassischer Fall des Computerbetrugs nach § 263a des deutschen Strafgesetzbuches (StGB).

Solche Taten sind aber nicht Anlass für Veranstaltungen wie heute. Das grenzenlose Internet hat nicht nur in Deutschland den Schwerpunkt verschoben. Jeder Täter kann überall auf der Welt mit Email und World Wide Web Straftaten verüben.

Die politischen Führer der Staaten in Europa haben dies erkannt. Am 23.11.2001 haben die Mitgliedstaaten des Europarates - nicht nur der Europäischen Union - die Convention on Cybercrime unterzeichnet. Die Convention ist am 01.07.2004 in Kraft getreten. Deutschland hat die Convention zwar unterzeichnet, aber noch nicht ratifiziert. Dennoch enthält das deutsche Strafrecht einige Vorschriften, die eine Verfolgung der Computerkriminalität ermöglichen.

1.1 Computerkriminalität im eigentlichen Sinn

Eine gesetzliche Definition gibt es in Deutschland nicht. Einzelne Paragrafen beziehen sich aber auf elektronische Daten oder Datenverarbeitungsanlagen (d.h. Computer). So lässt sich das Gebiet abgrenzen:

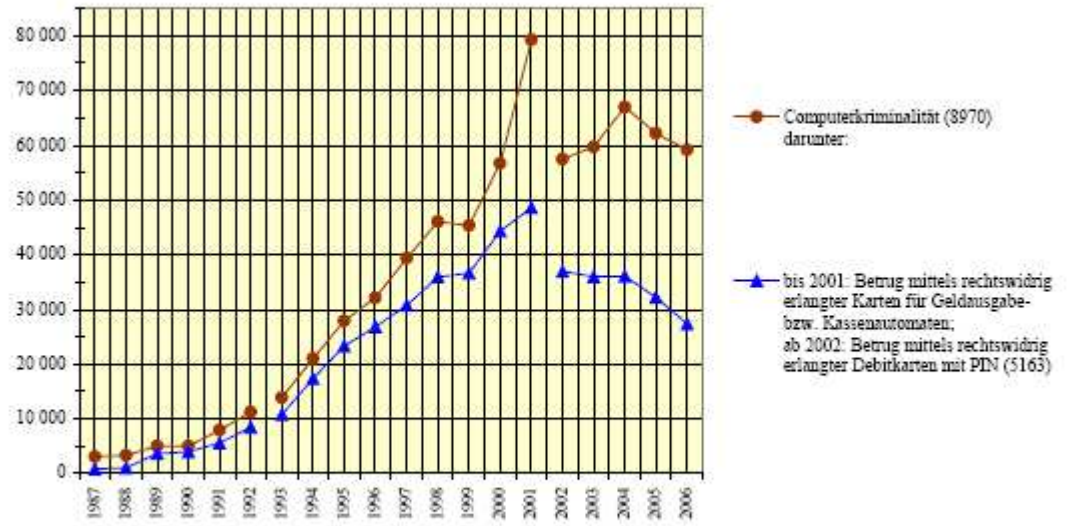
- Computerbetrug
- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung
- Datenveränderung, Computersabotage
- Ausspähen von Daten
- Softwarepiraterie
- Herstellen, Überlassen, Verbreiten oder Verschaffen sogenannter „Hacker-Tools“, welche darauf angelegt sind, „illegalen Zwecken zu dienen“

Die Cybercrime Convention enthält eine Definition, auf die man zurückgreifen kann:

- „computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
- “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

G96
erfasste Fälle

Computerkriminalität



Hinweis:
1987 – 1990: alte Länder
1991 – 1992: alte Länder mit Berlin
ab 1993: Bundesgebiet insgesamt
1998: Wegen zusätzlicher Aufnahme von Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (Schlüssel: 5179) ist ein Vergleich der Computerkriminalität (8970) zum Vorjahr beeinträchtigt.

Fallentwicklung und Aufklärung (Tabelle 01)
Bereich: Bundesgebiet insgesamt
T232

Schlüssel	Straftaten(gruppen)	erfasste Fälle		Aufklärungsquote	
		2006	2005	2006	2005
8970	Computerkriminalität	59 149	62 186	47,1	48,1
	davon:				
5163	Betrug mittels rechtswidrig erlangter Debitkarten mit PIN	27 347	32 232	40,6	40,9
5175	Computerbetrug -§263a StGB-	16 211	15 875	48,9	48,7
5179	Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	5 822	5 788	57,7	64,4
5430	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung -§§ 269, 270 StGB-	2 460	1 012	44,9	46,7
6742	Datenveränderung, Computersabotage -§§ 303a, 303b StGB-	1 672	1 609	29,0	35,9
6780	Ausspähen von Daten	2 990	2 366	43,8	42,2
7151	Softwarepiraterie (private Anwendung z.B. Computerspiele)	1 920	2 667	96,7	98,7
7152	Softwarepiraterie in Form gewerbsmäßigen Handelns	727	637	98,3	96,9

Quelle: PKS 2006, BKA (www.bka.de)

1.2 Computer als Tatwerkzeug - Mittel zum Zweck

Zur Computerkriminalität zählen weiter alle Delikte, bei denen die EDV zur Planung, Vorbereitung oder Ausführung eingesetzt wird. Beispielsweise kann der so genannte Ebay-Betrug ("klassischer" Betrug) nur mittels Computer und Internet begangen werden.

Schließlich wäre auch eine Körperverletzung, die mit einer Tastatur begangen wurde, hinzuzuzählen. Derartige Straftaten sind aber kein Problem der IT-Forensik.

2 Phishing

Als Phishing bezeichnet man Versuche, über gefälschte WWW-Adressen Daten eines Internet-Benutzers zu erlangen. Der Benutzer soll seine Zugangsdaten auf der vom Phisher präparierten Webseite preisgeben. Typisch ist die Nachahmung des Designs einer vertrauenswürdigen Organisation, um mit den Techniken des Social Engineering an „geldwerte“ Daten wie Benutzernamen und Passwörter für Online-Banking oder Kreditkarteninformationen zu gelangen. Phishing-Nachrichten werden oft auch per E-Mail versandt. Sie fordern den Empfänger auf, auf einer präparierten Webseite oder am Telefon geheime Zugangsdaten preiszugeben. Versuche, der wachsenden Anzahl an Phishing-Versuchen Herr zu werden, setzen unter anderem auf geänderte Rechtsprechung, Anwendertraining und technische Hilfsmittel.

Quelle: http://www.phishtank.com/stats/2007/07/

Nach einer Untersuchung durch BITKOM (Pressemitteilung vom 29.08.2007) hoben Täter im Jahr 2006 in mehr als 3.250 Fällen circa 13 Millionen Euro von den Konten der Opfer ab. Für 2007 wird erneut eine Steigerung um 25 % erwartet.

Phishing scheint mit einem Schaden von "nur" 13 Millionen Euro kein Problem zu sein. Kontoinhaber erleiden im Durchschnitt "nur" Verluste im unteren vierstelligen Bereich.

Dennoch wirft Phishing mehrere Fragen auf.

2.1 Erscheinungsform

Mit den „gestohlenen“ Zugangsdaten (Passwörter, Zugangsdaten für Online-Banking, Versandhäuser, Internet-Auktionshäuser, webbasierende Onlineberatungen oder Kontaktportale) kann ein (oder mehrere) Täter unter falscher Identität Leistungen in Anspruch nehmen oder Warengeschäfte tätigen. Soweit PIN/TAN-Informationen erlangt wurden, können unmittelbar Bankbewegungen veranlasst werden.

Um den Anschein zu erwecken, die Email stammen von einem bestimmten Unternehmen, werden Emailabsender benutzt, die denen der Unternehmen zum Verwechseln ähnlich sind. Zudem benutzen die Täter Logos und Markenzeichen der betroffenen Unternehmen. Absenderangaben werden verfälscht. Es werden auch Computer genutzt, die „gekapert“ wurden (im Rahmen sogenannter bot-Netze).

Aus juristischer Sicht sind verschiedene Abschnitte relevant:

- Erstellung einer „gefakten“ Webseite einer Bank o.ä., massenhafter Versand von Emails an eine Vielzahl existierender und nicht existierender Emailadressen (Spam),
- Eingabe der Zugangsdaten, i.d.R. von Kontonummer und PIN/TAN eines Bankkontos auf einer Webseite durch den (berechtigten) Bankkunden, der sich dazu durch „seine Bank“ aufgefordert sieht,
- Nutzung der Kontozugangsdaten zur Überweisung im Onlinebanking, i.d.R. auf das Konto eines inländischen Beteiligten,
- Transfer der Valuta i.d.R. über Western Union ins Ausland.
- Die Zahl der Täter ist unbestimmt. Ein einzelner Täter kann unter Umständen alle Abschnitte (nacheinander) begehen.

2.2 Anwendbare Strafvorschriften

Die genannten Phasen des Phishing sind aus juristischer Sicht im Detail umstritten, im Ergebnis kommt man aber grundsätzlich stets zu einer Strafbarkeit der beteiligten Täter.

2.2.1 Erstellen der Webseite, Versand der E-Mails

Vorbereitung eines Computerbetrugs (§ 263a Abs. 3 StGB): Gefälschte Websites zum Zwecke des „Phishing“ stellen keine Computerprogramme dar.

Fälschung beweiserheblicher Daten (§ 269 Abs. 1 StGB): Die Emailinformation (Absender u.a.) werden in den Spam- Emails verfälscht. Da der Rechtsverkehr (immer noch) auf die Echtheit vertraut, dürften diese Daten hinreichende Relevanz haben.

Ausspähen von Daten (§ 202a Abs. 1 StGB): Da der Geschädigte die Daten – wenn auch irrtümlich – selbst eingibt, ist der Tatbestand nicht erfüllt.

Computerbetrug (§ 263 a StGB): Der Versand der Email müsste dann als Beginn („jetzt geht es los“) der Tathandlung angesehen werden, nicht (nur) als Vorbreitungshandlung. Beim Versand der Spam-Email ist dem Versender der Empfänger nicht bekannt, eine Vielzahl der Mails geht auch ins Leere. Da zudem die Handlung des Opfers zwischengeschaltet wird, kann der Mailversand hierfür nur als – nicht strafbare – Vorbereitungshandlung gewertet werden.

Betrug (§ 263 Abs. 1 StGB): Das Versenden der Emails soll die Empfänger zur Preisgabe der Kontoinformationen bewegen. Aus Sicht der Täter ist damit schon alles getan, um diesen Erfolg herbeizuführen. Als Versuch eines Betrugs kann dies gewertet werden, wenn die Preisgabe der Kontoinformationen (PIN/TAN) mindestens zu einer sog. schadensgleichen Vermögensgefährdung führt (vergleichbar mit dem Verlust von EC-Karte und PIN). Da der Täter das Konto - sofern es nicht rechtzeitig gesperrt wird - ohne große Mühe mit Buchungen belasten kann, wird dies im Bezirk der Generalstaatsanwaltschaft Karlsruhe überwiegend bejaht.

Allerdings wird dabei außer Acht gelassen, dass neben einer Kontosperre Online-Buchungen oftmals innerhalb von bis zu 24 Stunden zurückgerufen werden können, eine endgültige Vermögensgefährdung eher fraglich sein dürfte (anders als bei der Verwendung von EC-Karte mit PIN, die sofort zu einer – verbürgten – Leistung der Bank führt).

Die Preisgabe der Kontodaten durch das Opfer führt dieser Ansicht nach zur Vollendung des Betrugs (Phase 2). Die folgende Nutzung (Phase 3) kann dann grds. nur als mitbestrafte Nachtat angesehen werden.

Markenrechtsverstöße (§ 143 Abs. 1 MarkenG): Die Täter verwenden Logos und Marken (Firmenname u.a.) der Banken und anderen Institute, die durchweg (z.T. auch international) markenrechtlich geschützt sind. Voraussetzung für eine Strafbarkeit ist aber, dass der Täter „im geschäftlichen Verkehr" handelt. Das Gegenteil des geschäftlichen Verkehrs stellen (nur) der sog. Amtsverkehr, der private Verkehr und der unternehmensinterne Verkehr dar, die ersichtlich beim Phishing nicht gegeben sind. Das Täterhandeln ist deshalb als „im geschäftlichen Verkehr" erfolgt anzusehen und nach MarkenG strafbar.

2.2.2 Eingabe der Daten

Der irrende Kontoinhaber ist nicht strafbar. Zivilrechtliche Haftungsfragen bleiben hier unberücksichtigt.

2.2.3 Missbrauch der Zugangsdaten

Da ihre Verwendung durch den Täter „unbefugt" erfolgt, erfüllt die Veranlassung von Transaktionen zu Lasten des Bankkunden den Tatbestand des **Computerbetrugs (§ 263a Abs. 1 Var. 3 StGB)**.

Im Einzelfall dürfte die Wertgrenze nach § 263 Abs. 4, § 248a StGB (Geringwertigkeit) stets überschritten sein. Allerdings dürften die Einzelfälle, die – soweit bekannt – nicht über 5.000 € liegen, einen bsd. schweren Fall begründen, soweit dem Täter Gewerbsmäßigkeit vorgeworfen werden kann. Soweit zusätzlich davon auszugehen ist, dass die Taten von einer Bande begangen wurde (§ 263 Abs. 5, § 263a Abs. 2 StGB), kommt der Verbrechenstatbestand in Betracht.

2.2.4 Weiterleitung der Gelder

Mit der Weiterleitung der Gelder werden Personen beauftragt, die im Inland ansässig sind und i.d.R. mit den Hintermännern nicht kollusiv zusammen arbeiten. Soweit die Inhaber dieser sog. Zielkonten

- gutgläubig sind (ihnen wird vorgegaukelt, es liege eine Überzahlung oder Fehlüberweisung vor), ist eine Strafbarkeit nicht gegeben.
- leichtfertig sich (um eine Provision zu erhalten) an der Weiterleitung des Geldes beteiligen, das aus einer Straftat stammt, kommt **Geldwäsche nach § 261 StGB** in Betracht.
- vorsätzlich dem Hintermann bei der Sicherung der Gelder durch Weiterleitung helfen, kommt **Beihilfe zum Computerbetrug (§§ 263a, 27 StGB)** in Betracht (so AG Hamm). Näher liegt aber in solchen Fällen Begünstigung (§ 257 StGB), wobei der Täter aber – was aber zu Nachweisproblemen führen kann – subjektiv die Absicht, dem Vortäter die Vorteile zu sichern, haben muss.
- aus Eigennutz (Provision), gar unter Anmeldung eines Gewerbes, als sog. Finanzagenten auftreten, kommt ein Vergehen nach **§ 54 KreditwesenG** in Betracht. Das (entgeltliche) Weiterleiten von Geldern stellt eine Finanzdienstleistung dar, die erlaubnispflichtig ist (->BAFin). Strafbar ist die Ausübung ohne Erlaubnis. Die Tat kann auch fahrlässig begangen werden. Wer „nur" im Finanzsektor im weiteren Sinne tätig ist, aber aufgrund seiner Geschäftstätigkeit nicht

den Bestimmungen des KWG unterliegt, bedarf der Makler-Erlaubnis gemäß § 34c GewO (Verstoß dagegen Ordnungswidrigkeit nach § 144 GewO).

3 Ermittlung der Tatsachen

Erhebliche Ermittlungsprobleme bringen die Phasen 1 und 4 mit sich, da sie (nur) im Ausland stattfinden und die Täter ihre Handlungen verschleiern.

Für das deutsche Strafprozessrecht ist das Legalitätsprinzip wesentlich. Bei – wie es in § 170 Abs. 1 StPO ausgedrückt wird – „genügendem Anlass" ist Klage zu erheben. Dies ist dann gegeben, wenn der Staatsanwalt nach Sach- und Rechtslage am Ende einer Hauptverhandlung zum Antrag auf Verurteilung gelangen würde. Bei der Prognose ist danach eine Bewertung der vorhandenen Beweismittel nach den für das Gericht geltenden Maßstäben erforderlich. Die dem Gericht vorzulegenden Beweismittel müssen rechtskonform erlangt und verwertbar.

Die zulässigen Maßnahmen der Strafverfolgungsbehörde sind in der Strafprozessordnung abschließend aufgezählt. Grundlegend ist das Recht der Strafverfolgungsbehörde, mit richterlichen Beschluss Wohnungen durchsuchen zu können. Dabei können sowohl Beweismittel als auch Vermögenswerte sichergestellt werden.

3.1 Phisher

Es liegt auf der Hand, dass Täter, die in der Ferne agieren, schwer zu ermitteln sind, Hinzu kommt, dass sie nicht persönlich in Erscheinung treten, sondern nur elektronisch.

Die Transaktion wird zwar bei der Bank gespeichert. Dabei fallen Daten an, die zurückverfolgt werden können. Wesentliche Spur ist die IP-Nummer.

Probleme ergeben sich aber,

- wenn die Tat eine lange oder auch kurze Zeit zurückliegt,
- Informationen zu IP-Nummern nicht gespeichert werden oder gelöscht werden,
- die Spur ins Ausland geht.

Von wenigen Ausnahmen abgesehen, über die in der Presse auch berichtet wurde, gelingt es nur in wenigen Fällen, Phisher aufzuspüren.

3.2 Finanzagent

Leicht zu ermitteln ist der in Deutschland ansässige Finanzagent. Sein Konto wird für die Überweisung benutzt. Über die Kontonummer kann er leicht identifiziert werden.

Die Staatsanwaltschaft hat auch das nötige Werkzeug, um schnell und effizient arbeiten zu können:

- umfassende Klärung der finanziellen Situation durch Auskünfte der Banken
- Vernehmung von Zeugen, auch zwangsweise
- Durchsuchung beim Täter (Finanzagent)
- Durchsuchung bei anderen Personen
- Beschlagnahme von Dokumenten, von Computern; ersatzweise Sicherung von Daten auch entfernter Computer (LAN, WAN, webspace)

- notfalls: Festnahme, Haftbefehl
- Gewinnabschöpfung (Vermögensbeschlagnahme)

4 IT-Forensik

Wenn Straftaten mit Computern begangen wurden, ergeben sich mannigfaltige Fragen. Es liegt auf der Hand, dass zur Beantwortung der Fragen Spezialisten herangezogen werden müssen. Auch unter Juristen ist dies eigentlich unstreitig.

Die Polizei in Baden-Württemberg hat hierfür bei allen größeren Polizeieinheiten (Polizeidirektionen) Auswertetrupps eingerichtet, die so genannten DVE-Stellen. Sie sind, wie die Erfahrung zeigt, in der Lage schnell und effizient zu arbeiten.

Bei speziellen Fragen werden auch externe Sachverständige hinzugezogen.

Digitale Forensik ist die Aufbereitung von kriminellen Vorfällen im Zusammenhang mit Computern, zur Beweissicherung und zur Feststellung des Täters. Um Beweise zu sichern, werden z.B. Festplatten analysiert und Protokolle des Netzverkehrs gesichert.

Die Fragen sind dabei immer die gleichen.

Wie erhielt der Angreifer Zugriff auf das Netzwerk?

Von wo ging der Angriff aus?

Wer hat den Angriff durchgeführt?

Was war das Ziel des Angreifers?

Welche Änderungen am System wurden vorgenommen?

Ein Problem ist, dass der Geschädigte – unbewusst – Spuren vernichten kann. Oft kann der Angriff nicht weiter beobachtet oder zugelassen werden. Sinnvolle Maßnahmen zum Schutz verändern das Originalsystem. Der Nachweis der Tat wird so schwierig.

4.1 Ermittlungen in Datennetzen

Unabhängig von konkreten Ermittlungen wird anlassunabhängig im Internet recherchiert. In Baden-Württemberg ist dafür das Landeskriminalamt zuständig. Ziele sind Kinderpornografie, Extremismus und Terrorismus.

Wichtig zur Verfolgung sind dabei ausreichende Spuren. Im Internet sind dies logischerweise unter anderem die Verbindungsdaten. Diese werden in Log-Files gespeichert, die allerdings derzeit nur wenige Tage vorgehalten werden.

Bis zur Verkürzung der Speicherfrist durch die Deutsche Telekom von 90 Tagen auf 7 Tage – was gesetzeskonform ist – konnte der Spur IP-Nummer nachgegangen werden – jedenfalls im Inland. Derzeit ist dies problematisch, da – sofern überhaupt gespeichert wird – Ermittlungen nicht stets in der zur Verfügung stehenden Zeit erfolgen können.

Die angekündigte Vorratsdatenspeicherung, die mit sechs Monaten angemessen ist, wird Abhilfe bringen.

4.2 Ermittlungen in lokalen Computern

Einfacher sind die Ermittlungen, wenn ein Computer (oder anderes System) sichergestellt wurde. Die Beschlagnahme mit richterlichem Beschluss erfolgt gegebenenfalls nach einer Durchsuchung. Die Rechtslage ist eindeutig.

Die Auswertung erfolgt dann in der Regel durch die Polizei – die genannten Sachbearbeiter für DV-Unterstützung in Ermittlungsverfahren. Unter Einsatz der bekannten Techniken und Software können die Systeme und Datenträger ausgewertet werden.

Aber auch hier zeigen sich erste Problemfelder:

- Zugangssperren
- Verschlüsselung der Daten
- große Speicherkapazitäten
- vernetzte Systeme, die lokal nicht mehr arbeitsfähig sind.

5 Rechtsfragen bei privaten Ermittlungen

Es gibt neben den in den polizeilichen Statistiken erfassten Computercrime-Fällen auch viele Taten, die nicht bekannt werden. Es gibt Taten, die nur den Beteiligten bekannt sind, aber nicht staatlichen Stellen. Gründe für eine Nichtanzeige können sein:

- vermuteter Image- und Vertrauensverlust bei Bekannt werden in der Öffentlichkeit.
- relativ gering ausgeprägtes Interesse an einer Strafverfolgung; zivilrechtliche Ansprüche stehen im Vordergrund.
- Unternehmen ziehen es u. U. vor, eigene Mitarbeiter (m/w), die Täter eines entsprechenden Delikts sind, ohne Einschaltung der Strafverfolgungsbehörden selbst zu sanktionieren.
- fehlendes Vertrauen in die Fach- und Sachkenntnis der Strafverfolgungsbehörden.
- Nichterkennen der Verletzung eigener Rechte oder des eigenen Vermögens.

An der Klärung der Taten besteht dennoch großes Interesse. Dazu werden Fachleute auf dem Gebiet der IT-Forensik eingesetzt.

Hier stößt man dann auf Aussagen wie folgende: „Wie kompliziert die Sachlage ist, mag das Detail zeigen, dass Forensiker sich strafbar machen, wenn sie bei ihrer Detektivarbeit auf Kinderpornografie stoßen und diese nicht zur Anzeige bringen, weil sie an einem anderen Fall "dran" sind.“

Zunächst ist darauf hinzuweisen, dass es eine Pflicht nicht gibt, jede Straftat anzuzeigen. Es kommt darauf an, welche Position man hat und welche Straftat es ist:

- Für Amtsträger, die im Bereich der Strafverfolgung tätig sind (Staatsanwalt, Polizeibeamter) die dienstlich von strafbaren Sachverhalten erfahren: es besteht eine Anzeigepflicht.
- Für Staatsbedienstete außerhalb des Bereichs, der den Amtsträgern der Strafverfolgung zugewiesen ist, besteht keine allgemeine Pflicht, ihnen bekannt gewordene Straftaten anzuzeigen. Dies gilt – erst recht – für Privatpersonen.

- Jedermann, d.h. auch IT-Forensiker, müssen schwere Straftaten nach § 138 StGB anzeigen. § 138 StGB betrifft aber nicht die klassischen IT-Delikte (Ausspähen von Daten, Datenveränderung, Computersabotage, Urheberrechtsdelikte) oder Kinderpornografie. Gemeint sind Vorbereitung eines Angriffskrieges, Landesverrat und Gefährdung der äußeren Sicherheit, Geldfälschungstatbestände, Totschlag, Mord und Völkermord, Menschenraub, Verschleppung, erpresserischer Menschenraub, Geiselnahme sowie Menschenhandel, Raub- und Erpressungsdelikte, gemeingefährliche Straftaten, die Bildung einer terroristischen Vereinigung.
- Die Tat muss anzeigt werden, solange die Ausführung oder der Erfolg noch abgewendet werden kann.
- Die Anzeige kann gegenüber einer Behörde oder gegenüber dem Bedrohten erfolgen.
- Weitere Rechtsfragen (Beihilfe, Begünstigung, Strafvereitelung) spielen im Kontext IT-Forensik keine wesentliche Rolle.

5.1 Private Investigation

Die „private investigation“ hat wie die Ermittlungsarbeit der Strafverfolgungsbehörden das Ziel, einen Sachverhalt nachvollziehbar und nachweislich aufzuklären. Es ist Aufgabe der staatlichen Strafverfolgungsbehörden, den Sachverhalt – einschließlich der entlastenden Umstände – vollständig aufzuklären. Deshalb kann die Staatsanwaltschaft die Ermittlungen nicht an den Geschädigten oder an ein Privatunternehmen delegieren oder „outsourcen“. Die Strafverfolgungsbehörden sind aber nicht nur bereit, sondern wegen ihres Auftrages zur Sachverhaltsaufklärung auch gezwungen, die vom Geschädigten vorgelegten Beweise zur Kenntnis zu nehmen und zu bewerten.

Im Gegensatz zu den staatlichen Stellen sind private Ermittler grundsätzlich nicht an die Regularien der Strafprozessordnung gebunden (z.B. Beteiligung des Verteidigers). Ebenso müssen private Ermittler den Beschuldigten nicht über seine Rechte belehren. Selbst eine Täuschung als verbotene Vernehmungsmethode (§ 136a StPO) ist möglich.

Private Ermittler können auch Telefongespräche durch andere Personen mithören lassen.

Die Strafverfolgungsbehörden dürfen solcher Beweise aber nicht verwenden.

Private Ermittler haben schließlich einen großen Vorteil. Sie können ohne weiteres im Ausland tätig werden. Sie benötigen im Regelfall keine Zulassung durch staatliche Stellen.

5.2 Strafbarkeit des „weißen“ Hackers

Internationale Vereinbarungen wie die Cybercrime Convention und der EU-Rahmenbeschluss 2005/222/JI (Justiz/Inneres) vom 24. Februar 2005 zwingen die Vertragsstaaten, ihr nationales Strafrecht anzupassen. In Deutschland bestanden schon seit einigen Jahren Strafbestimmungen gegen Computerkriminalität. Mögliche Strafbarkeitslücken und die genannten Verträge haben zu Verschärfungen der geltenden Vorschriften und zu neuen Paragrafen geführt. Das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 07.08.2007 (BGBl. I 2007 S. 1786, veröffentlicht am 10.08.2007, in Kraft getreten am 11.08.2007) enthält aber keine Vorschrift, die das Phishing als solches eindeutig unter Strafe stellt.

Der geänderte § 202a StGB stellt nun auch das (bloße) Eindringen in einen fremden, irgendwie gesicherten Rechner unter Strafe - jedenfalls wenn es unbefugt erfolgt. Ein Hacker, der aus Lust am Experiment loslegt, dürfte Probleme bekommen. Die Ausrede, man wolle nur Sicherheitslücken aufdecken, zieht nicht mehr. Unproblematisch bleibt das Hacking mit Auftrag des Eigentümers des Computers.

Von besonderer Bedeutung ist der neue § 202c StGB: er stellt das Vorbereiten des Ausspähens und Abfangens von Daten unter Strafe. Diskutiert wird, ob nun auch der bloße Besitz von "Schadprogrammen" strafbar sein kann. Absatz 1 Ziffer 2 lautet (auszugsweise): "Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft."

Der neue Straftatbestand, der – vergleichbar § 263a Abs. 3 StGB – klassische Vorbereitungshandlungen unter Strafe stellt, erfasst die fraglos strafwürdige Praxis, Hackertools unter dem Mantel der Berichterstattung oder Forschung allein zum Zwecke der Begehung von Straftaten anzubieten. Allerdings dürfte dies nur in wenigen Fällen zum Tragen kommen, da die überwiegende Zahl der „Tools“ mehreren Zwecken dienen kann. Zudem wird nach dem Wortlaut auch notwendige Berichterstattung („sonst zugänglich macht“) unter Strafe gestellt, ohne dass dies angezeigt wäre.

Ausgehend von den Vorgaben der Cybercrime Convention muss der Zweck eines Programms anhand von Kriterien bestimmt werden. Entscheidend ist das Missbrauchspotential. Kann ein Computerputerprogramm sowohl für strafbare Vorbereitungshandlungen als auch zu legitimen Zwecken eingesetzt werden, muss geprüft werden, welche der Verwendungsmöglichkeiten überwiegt. Auch der konkrete Einsatzzweck (berufsmäßiger Einsatz im Rahmen eines Untersuchungsauftrags) muss berücksichtigt werden. Computerprogramme, deren mögliche strafbare Zweckentfremdung nur ein ungewollter Nebeneffekt ist, können so weiter genutzt werden.

Was den Betroffenen wenig helfen wird: endgültige Klarheit wird erst die Rechtsprechung bringen. Jedenfalls ist der bloße Besitz von Hackertools nicht strafbar.

6 Probleme bei staatlichen Ermittlungen

Immer wieder hört oder spricht man von Problemen, die die Strafverfolgungsbehörden haben. Oft sind dabei fehlende Mittel (Geld, Personal) oder die Zeit gemeint. Manchmal wird die Gesetzeslage beklagt, obwohl die Verfassung die Strafverfolgungsbehörden an Recht und Gesetz bindet. Wünsche und Hoffnungen sollten keine Rolle spielen. Diese Diskussion führen letztlich die Politiker.

Dennoch gibt es gesetzliche Beschränkungen. Oftmals werden dadurch Ermittlungen oder die Durchsetzung der Rechte der Geschädigten erschwert.

6.1 Rechtshilfe

Merkmal der IT-Kriminalität ist, dass der Aufenthalt von Täter und Opfer, die Tatbegehung oder der Eintritt eines Schaden (Taterfolg) nicht an bestimmte Orte gebunden sind, sondern vielmehr „world wide“ statt finden.

Auch bei Online-Taten ist allerdings die Zuständigkeit deutscher Behörden gegeben, wenn

- der Tatort in Deutschland liegt,
- der Täter Deutscher ist,
- das Opfer Deutscher ist oder
- dass Weltrechtsprinzip Anwendung findet (z.B. Kinderpornografie).

Bei Auslandsbezug sind staatliche Maßnahmen nur unter Nutzung der Rechtshilfe zulässig; bei Ermittlungen im Ausland gelten die allgemeinen Regelungen. „Erleichterungen“ für IT- Ermittlungen sind dünn gesät.

Die "Ministerkonferenz der G-8-Staaten zur Bekämpfung transnationaler organisierter Kriminalität" hat am 19. und 20. Oktober 1999 in Moskau Grundsätze betreffend den grenzüberschreitenden Zugriff auf gespeicherte Computerdaten beschlossen. Vereinbart wurde (Auszug):

> 1. Jeder Staat stellt sicher, dass er in der Lage ist, für eine schnelle Sicherung von Daten zu sorgen, die in einem Computersystem gespeichert sind.
>
> 2. Ein Staat kann einen anderen Staat ersuchen, für eine schnelle Sicherung von Daten zu sorgen, die in einem Computersystem gespeichert sind, das sich in diesem anderen Staat befindet.
>
> 3. Der ersuchte Staat trifft nach Maßgabe seines innerstaatlichen Rechts alle geeigneten Maßnahmen, um diese Daten schnell zu sichern.
>
> 4. Ein förmliches Ersuchen soll so schnell wie möglich erledigt werden.
>
> 5. Jeder Staat nimmt Rechtshilfeersuchen über schnelle, aber zuverlässige Kommunikationsmittel einschließlich mündlicher Übermittlung, per Fax oder E-Mail, soweit erforderlich, mit anschließender schriftlicher Bestätigung entgegen und beantwortet sie entsprechend.
>
> 6. Ein Staat muss die Genehmigung eines anderen Staates nicht einzuholen, wenn er
>
> a) auf öffentlich zugängliche Daten (offene Quellen) zugreifen will, gleichviel, wo die Daten geographisch belegen sind;
>
> b) auf Daten, die in einem im Ausland belegenen Computersystem gespeichert sind, zuzugreifen oder diese Daten festzustellen, zu kopieren oder zu erheben, vorausgesetzt, er wird mit der rechtmäßigen und freiwilligen Zustimmung einer Person tätig, die rechtmäßig befugt ist, ihm diese Daten offen zu legen.

In der Praxis scheitert die schnelle Umsetzung an vielem. Es gibt Sprachbarrieren. Die Strafverfolgungsbehörden werden oft zu spät eingeschaltet. Die Strafvorschriften sind in den einzelnen Staaten noch immer unterschiedlich. Zudem bestehen unterschiedliche Verfolgungsgrundsätze.

So zwingt das Legalitätsprinzip in Deutschland auch bei Kleinbeträgen zum Handeln. Oftmals wird auch bei Kleinstbeträgen (vgl. Ladendiebstahl) staatliches Handeln verlangt. In diesem Zusammenhang kann auch die Praxis der Vertreter der Urheber erinnert werden, massenhaft Anzeigen gegen File-sharing-Nutzer zu erstatten. Dem gegenüber können die Strafverfolgungsbehörden anderer Staaten nach eigenem Ermessen entscheiden, ob sie gegen einen Straftäter vorgehen. So könnte eine niederländischer Staatsanwalt auch bei einem Betrug über 70.000 Euro von Ermittlungen absehen - in Deutschland undenkbar. Ähnlich ist die Lage in Frankreich.

6.2 Cyber Crime Convention

Die Cybercrime Convention (CETS Nr. 185) stellt einen weiteren Schritt auf grenzüberschreitende Ermittlungen dar. Sie ist zwar kein nationales Recht. Sie wird aber von immer mehr Staaten umgesetzt.

In ihrer lesenswerten Präambel haben die Staaten des Europarates die Ziele genannt. Neben einer besseren Strafverfolgung sollen auch die Rechte der Bürger - auch gegen staatliche Maßnahmen - geschützt werden.

Die Cybercrime Convention legt in den einzelnen Artikeln fest, was die Vertragsstaaten umsetzen müssen. Neben der Bekämpfung der "klassischen" Computer-Kriminalität sind die Kinderpornografie und Verstöße gegen das Urheberrecht genannt.

6.3 Ausblick: Online-Durchsuchung

Vor der Jahrtausendwende war Orwells Überwachungsstaat "1984" eine Gefahr, die durchaus ernst genommen wurde. Datenschutz (und Datensicherheit) waren ein hohes Gut.

Die in den USA am 11. September 2001 verübten Terrorangriffe haben aber zu einer neuen oder zumindest erweiterten Definition des Begriffes Terrorismus geführt. So ist es nun mehr ausgeschlossen, Computerkriminalität als terroristischen Akt zu betrachten. Nicht nur in den USA ist es denkbar, Überwachungen der Telekommunikation ohne Zustimmung eines Richters vorzunehmen oder DNA-Fingerabdrücke" von Computerstraftätern zu sammeln und wie die von Mördern oder Entführern zu speichern.

Nach geltendem Recht können die Strafverfolgungsbehörden Durchsuchungen von Wohnungen vornehmen. Computer in Deutschland können problemlos sichergestellt werden (die Auswertung ist oft zeitaufwändig.) Auch auf so genannte Anonymisierungsserver kann zugegriffen werden (LG Konstanz, MMR 2007 S. 193). Ein Täter kann verhaftet werden. Die (gesamte) Telekommunikation kann in Echtzeit überwacht werden. Dazu stehen Ermittlungsmöglichkeiten wie der Einsatz von verdeckten Ermittlern, die Rasterfahndung, die Postbeschlagnahme und die Wohnraumüberwachung ("Lauschangriff") zur Verfügung.

Gesetzlich nicht geregelt ist eine „Online-Durchsuchung“, die verdeckt durchgeführt wird (Trojaner / Remote-Steuerung, Keylogger). Ihre Einführung ist in der Diskussion (siehe Entwurf eines Änderungs-Gesetzes zum BKA-Gesetz zur „Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt“). Entfernte PC sollen auf verfahrensrelevante Inhalte hin durchsucht werden, ohne dass die Polizei selbst am Standort des Geräts ist (Leipold, K.: Die Online-Durchsuchung, NJW-Spezial 2007 S. 135). Technische und rechtliche Einzelheiten sind umstritten.

Technisch kann die Software zur Online-Durchsuchung (z.B. Trojanisches Pferd) die IT-Sicherheit aushöhlen. Der Missbrauch der Technik durch Unbefugte kann nicht ausgeschlossen werden (Mitarbeiter der Dienste, fremde Mächte, Kriminelle). Die bislang bekannten geplanten Maßnahmen erfüllen nicht die Anforderungen, die bislang an eine gerichtsfeste Beweisaufnahme gestellt werden (v.a. Sicherung des Original-Datenbestands, Auswertung von Kopien). Allenfalls eine Hardware-Lösung (Keylogger) könnte gerichtsfest nachvollzogen werden.

Juristisch entsprechen die bisher vorgetragenen Begründungen zur Notwendigkeit einer Online-Durchsuchung nicht den verfassungsrechtlichen Kriterien, die angesichts der Schwere des Eingriffes in die Grundrechte beachtet werden müssen. Offen sind folgende Fragen: Welcher Verdachtsgrad muss gegeben sein (Anfangsverdacht,

hinreichender oder dringender Tatverdacht)? Wie schwer muss die Tat sein (Strafrahmen oder konkreter Schuldvorwurf, "nicht unerheblich")? Wer darf die Maßnahme anordnen (Richtervorbehalt, Gefahr im Verzug)? Gefahrenabwehr oder Geheimdienst oder Strafverfolgung? Wie sollen die Rechte des Beschuldigten (z.B. Schweigerecht) angemessen berücksichtigt werden?

7 Ausblick

Sicher ist, dass bestimmte Täter auch zukünftig von den Strafverfolgungsbehörden (und von privat beauftragten IT-Forensikern) ermittelt werden. Ob es nur die im Cartoon von Ritsch & Renn

> *http://www.heise.de/ct/schlagseite/06/20/gross.jpg*
>
> *"Grüß Gott. Ich komme von der Deutschen Bank. Immer wieder versuchen Gauner über fingierte E-Mails Kontoinformationen zu erlangen. Der neueste Trick ist, dass Leute, die offensichtlich keine Bankmitarbeiter sind von Tür zu Tür gehen, um Kontodaten auszuspähen. Deshalb mussten wir Ihre Konten umstellen. Geben Sie mir bitte alle Ihre Sparbücher, damit wir diese kostenlos für Sie aktualisieren können."*

dargestellte Tätergruppe ist, wird die Zukunft zeigen.

8 Literatur

Böckenförde, T.: Die Ermittlung im Netz, 2003

Borges, G.: Rechtsfragen des Phishing - Ein Überblick, NJW 2005, S. 3313

Buggisch, W; Kerling, C.: „Phishing“, „Pharming“ und ähnliche Delikte. Erscheinungsformen und strafrechtliche Bewertung, Kriminalistik 2006, S. 531

Ernst, S.: Arbeitsrechtliche Fragen in (Ernst, S., Hrsg.) Hacker, Cracker & Computerviren, 2004, S. 263

Ernst, S.: Das neue Computerstrafrecht, NJW 2007 S. 2661

Gercke, M.: Die Strafbarkeit von "Phishing" und Identitätsdiebstahl - Eine Analyse der Reichweite des geltenden Strafrechts, CR 2005, S. 606

Geschonneck, A.: Computer-Forensik, 2. Aufl. 2006

Gruhl: "Grenzenlose" Ermittlungen im Internet? in (Welp, J., Hrsg.) kriminalität@net, 2003, S. 49

Gruhl, J.: Datenverarbeitung in (Müller- Gugenberger, C.; Bieneck, K., Hrsg.) Wirtschaftsstrafrecht, 4. Aufl. 2006

Gruhl, J.: Nicht nur Geheimagenten leben gefährlich - sondern auch "Finanzagenten". Anmerkung zum Urteil des Amtsgerichts Hamm vom 5.9.2005 - 10 Ds 101 Js 244/05-1324/05, JurPC Web-Dok. 91/2006

Hansen, M.; Pfitzmann, A.; Roßnagel, A.: Online- Durchsuchung, DRiZ 2007, 225

Heghmanns, M.: Strafbarkeit des "Phishing" von Bankkontendaten und ihrer Verwertung , wistra 2007, 167

Hofmann, M.: Die Online-Durchsuchung - staatliches „Hacken“ oder zulässige Ermittlungsmaßnahme? NStZ 2005, S. 121

Kutscha, M.: Verdeckte „Online-Durchsuchung“ und Unverletzlichkeit der Wohnung, NJW 2007 S. 1169

Marberth-Kubicki, A.: Computer- und Internetstrafrecht, 2005

Popp, A.: "Phishing", "Pharming" und das Strafrecht, MMR 2006, S. 84

Schomburg, W.; Lagodny, O.; Gleß, S.; Hackner, T: Internationale Rechtshilfe in Strafsachen. International Cooperation in Criminal Matters. 4. Aufl. 2006

Schultz, A.: Neue Strafbarkeiten und Probleme - Der Entwurf des Strafrechtsänderungsgesetzes (StrafÄndG) zur Bekämpfung der Computerkriminalität vom 20.09.2006, MIR 2006, Dok. 180, Rz. 1-52

Störing, M.: Strafprozessuale Zugriffsmöglichkeiten auf E-Mail-Kommunikation, 2007

Werner, D.; Borges, G.: Anmerkung zu AG Hamm, Urt. v. 05.09.2005 - Strafbarkeit eines Finanzagenten, CR 2006, 71

Willer, C.; Hoppen, P.: Computerforensik - Technische Möglichkeiten und Grenzen, CR 2007 S. 610

9 Zum Autor

Oberstaatsanwalt (Ständiger Vertreter des Leitenden Oberstaatsanwalts) bei der Staatsanwaltschaft Konstanz. Leiter einer Ermittlungsabteilung (betreffend Betäubungsmittel- und Organisierte Kriminalität, Geldwäsche Korruption, Geldfälschung, Verstöße gegen das Kriegswaffenkontrollgesetz). Leiter der Strafvollstreckungsabteilung. Pressesprecher.

Seit 1986 im Justizdienst des Landes Baden-Württemberg als Richter und Staatsanwalt 1992 - 1995 Vorsitzender Richter am Landgericht Leipzig. 2001 - 2004 Leiter des Referates Organisation im Justizministerium Baden-Württemberg.

Autor zum Wirtschafts- und Computerstrafrecht.

Internet: www.gruhl.de