Onlinedurchsuchung. Bundestrojaner

Das Cybercrimerecht weist erhebliche Lücken auf

Cyberfahnder #1

Mit seinem Beschluss vom 31.01.2007 – StB 18/06 [1] - hat der Bundesgerichtshof entschieden, dass die "verdeckte Online-Durchsuchung" mangels einer Ermächtigungsgrundlage unzulässig sei. Er stellt sich damit gegen die vom Generalbundesanwalt – GBA – vertretene Auffassung, diese Ermittlungshandlung ließe sich aus der allgemeinen Ermächtigungsgrundlage des § 102 StPO zur Durchsuchung beim Verdächtigen ableiten.

Während der BGH immer nur von der „Online-Durchsuchung“ spricht, war in der Presse sehr schnell die Rede von dem „Bundestrojaner“. Seine erste Erwähnung erfolgte in der Süddeutschen Zeitung am 07.12.2006 [2], die damit die Spekulationen darüber eröffnete, wie er eingesetzt werden kann und wie er funktioniert. Sie bemühte dazu einen Fachmann von der anerkannten Computerzeitschrift **c't**, der die beiden nahe liegenden Methoden zur Einschleusung von Spionagesoftware referierte: Entweder nutzen die Ermittlungsbehörden eine Sicherheitslücke in Standard-Betriebssystemen oder -Programmen aus oder sie verwenden einen Trojaner, den sie der Zielperson im Zusammenhang mit anderen Dateien präsentieren und unter schieben. Das erste wäre ein klassischer Hacking-Angriff und das zweite ein ebenso klassischer Angriff mit Malware als Anlage zu einer E-Mail oder per Download von einer Website, zu der die Zielperson von den Ermittlungsbeamten ge- und verführt werden müsste.

In der folgenden Debatte meldete sich auch die Firma Microsoft, die bestritt, dass sie Vereinbarungen mit staatlichen Stellen über Hintertüren in ihrer Software getroffen habe oder dass die Sicherheitslücken in ihren Produkten ausgenutzt werden könnten [3]. An anderer Stelle äußerte sich der Hersteller von Antivirenprogrammen, Kaspersky, mit der Einsicht, dass staatliche Spionageprogramme an modernen Schutzprogrammen scheitern würden [4].

Beide Aussagen sind einfach zu widerlegen und reines Marketing zum Schutz und zur Förderung der eigenen Produkte auf dem Markt. Natürlich eignen sich Microsofts immer wieder bekannt werdenden Sicherheitslücken zum Eindringen in fremde IT-Systeme und die kommerziellen Antivirenprogramme sind auf die Abwehr von Malware ausgerichtet, die massenhaft verbreitet wird. Sie scheitern an den Unikaten, die zum gezielten individuellen Angriff im Bereich der Industriespionage verwendet werden.

heise online meldete schließlich, dass die Bundesregierung die Entwicklung des Bundestrojaners mit kräftigen Finanzmitteln fördere [5].

Telepolis entlarvte die publizistische Diskussion als ohne Substanz und Realität [6] und brachte zu guter Letzt SINA ins Spiel: Diese vom Bundesamt für Sicherheit in der Informationstechnik – BSI – entwickelte und geförderte Sicherheitstechnik für gewerbliche und behördliche Technik könne mit einer einfachen Erweiterung für staatliche Spionageangriffe erweitert werden [7].

Hier irrt Telepolis: Die Techniken zur Industriespionage, die zum Einsatz kommen würden, sind längst gebräuchlich, erprobt und ihre Anpassung an individuelle Bedürfnisse wird in kriminellen Foren öffentlich angeboten – einschließlich der Aufschläge für einen zeitlich befristeten Support [8]. SINA hingegen ist eine Sicherheitstechnik, deren Kosten sich nur für mittlere und große Unternehmen und Behörden lohnen. Das BSI hat einen Namen zu verlieren und wird in diese Technik keine Hintertüren einbauen, die grundsätzlich auch von Kriminellen missbraucht werden könnte.

---

1 BGH, Beschluss vom 31.01.2007 – StB 18/06.

2 Jörg Donner, Bundestrojaner im Computer. Ein unvorsichtig geäußerter Gedanke im Chat könnte in Zukunft einen Besuch des Bundeskriminalamtes zur Folge haben..., SZ 07.12.2006.

3 Süddeutsche Zeitung ebenda.

4 Kaspersky hält ebenfalls nicht viel vom Bundestrojaner, tecchannel 11.12.2006.

5 Zwei Programmierstellen für den "Bundestrojaner", heise online 11.01.2007.

6 Burkhard Schröder, Verdeckter Zugriff auf Festplatten, Telepolis 06.02.2007.

7 Volker Birk, Der Staat als Einbrecher: Heimliche Online-Durchsuchungen sind möglich, Telepolis 03.03.2007.

8 Moritz Jäger, Das Netz der Phisher: Wie Online-Betrüger arbeiten, tecchannel 20.09.2006; Jürgen Schmidt, Die Super-Trojaner. So arbeiten moderne Schädlinge, c't 2/07, Seite 86; Axel Kossel, Markus Kötter, Piraten-Software. Wenn Schadprogramme den PC kapern, c't 2/07, Seite 76.

Unverletzlichkeit der Wohnung

Zunächst der Ermittlungsrichter beim BGH [9] und auf die Beschwerde des GBA der zuständige Senat hatten über eine technische, über eine Datennetzverbindung betriebene Ausforschung in der privaten Wohnung des Beschuldigten zu entscheiden. Beide haben die Anordnung mangels einer gesetzlichen Ermächtigung für diese Eingriffshandlung abgelehnt.

Anders als das Bundesverfassungsgericht – BVerfG – in seiner wichtigen Entscheidung über die Behandlung von Verkehrsdaten nach Abschluss des Übertragungsvorgangs [10], das das Grundrecht auf informationelle Selbstbestimmung als Ermessensmaßstab für die Anwendungsgrenzen des allgemeinen Strafverfahrensrechts hervorgehoben hat, legt der BGH seiner Entscheidung das Fehlen einer vom Gesetzgeber gewollten und geregelten Eingriffsbefugnis zugrunde. Mit den Besonderheiten des grundrechtlichen Schutzes aus Art. 13 Grundgesetz über die Unverletzlichkeit der Wohnung setzt er sich nicht auseinander, obwohl er umfassend über die bereits vom Gesetzgeber zugelassenen Eingriffsmaßnahmen in den privaten Lebensbereich referiert [11].

Das BVerfG und der BGH haben im Zusammenhang mit der strafverfahrensrechtlichen Durchsuchung noch keine Klarheit darüber hergestellt, wie weit der besondere Schutz der Wohnung als Ort der Privatsphäre reicht. Damit bleibt der Bereich zwischen dem (bewusst) öffentlichen Handeln von Personen und ihrem Rückzug in einen nicht antastbaren Privatbereich unklar.

Eine Kapitalgesellschaft ist eine juristische Person und genießt damit den Schutz des Eigentums aus Artikel 14 Grundgesetz. Der besondere Schutz der Familie (Art. 6 GG) kann für sie denklogisch nicht gelten und eine besondere Privatsphäre mit der Qualität einer Wohnung als Rückzugsbereich von der Öffentlichkeit kommt für sie auch nicht in Betracht.

Was ist mit den Ladenlokalen von Einzelkaufleuten oder den Arbeitszimmern von Nebenerwerbstätigen? Beide Räumlichkeiten dienen nicht dem Rückzug ins Private, sondern zum Geldverdienen in der Öffentlichkeit. Sind sie dennoch Wohnungen im Sinne von Artikel 13 Grundgesetz? [12]

Formen der Online-Kriminalität

Auch wenn der BGH über die Online-Durchsuchung als solches entschieden hat, so entschied er nur über den besonderen Schutz der EDV-Anlage des Beschuldigten in seiner Wohnung und damit in dem tiefsten privaten Rückzugsbereich. Ihm ist zu Gute zu halten, dass er den Eingriff in diesen Bereich nicht prinzipiell aus Verfassungsgründen ausgeschlossen hat, sondern an einer besonderen gesetzgeberischen Ermächtigung scheitern ließ.

Die äußeren Umstände für hoheitliche Eingriffshandlungen über Datennetze sind hingegen vielfältig und hinterlassen einen hohen Grad an Unsicherheit.

1) **öffentlich gewidmete Privatbereiche**
   Gewerblich genutzte Orte und Plattformen im Internet – hier im Sinne von Tagebüchern, Blogs und zugangsbeschränkten Webseiten – bedürfen eines geringeren Schutzes vor der Strafverfolgung als der tiefe private Rückzugsbereich, die Wohnung. Insoweit ist weder Art. 13 GG über die Unverletzlichkeit der Wohnung noch das Recht auf Informationelle Selbstbestimmung vollständig wirksam, sondern beide immer nur mit der Einschränkung, dass die öffentliche Präsentation gewollt und der Rückzug ins Private jedenfalls teilweise aufgegeben wurde.
2) **zugangsgeschützte Internetauftritte**
   Portale, Foren und Newsgroups, die sich nur einer beschränkten, aber persönlich unbekannten (konspirativen) Öffentlichkeit öffnen, geben ihren privaten, ganz individuellen Interaktionsbereich bewusst auf und bieten den Zugang zu noch unbekannten Gleichgesinnten. Sie verdienen keinen besonderen Schutz der Glaubens- und Meinungsfreiheit (Art. 4, 5 GG).

   In diesen Fällen macht es Sinn, Ermittlungshandlungen nicht von vornherein auszuschließen, sondern einer nachträglichen Inhaltsbewertung zu unterziehen, die die Frage der Verwertbarkeit für die Tatfeststellungen klärt.

9 Beschluss vom 25.11.2006 - 1 BGs 184/2006.
10 Urteil vom 02.03.2006 - 2 BvR 2099/04.
11 Oben Fußnote 1, Randnummer 12.
12 Mit der Rechtsprechung des BVerfG ist diese Frage zu bejahen. Es sieht auch Kanzlei- und gewerblich genutzte Räume als Wohnungen an. Zuletzt Beschluss vom 07.09.2006 – 2 BvR 1141/05.

3) **Auslagerung privater Daten**
Wer bewusst seine privaten Daten in der Öffentlichkeit präsentiert und das womöglich auch zugangsgeschützt, kann keinen Schutz vor der Strafverfolgung verlangen. Dies gilt ganz besonders für Online-E-Mail-Dienste wie web.de und gmx.de. Wer seine Korrespondenz online von allen möglichen Orten aus empfangen, bearbeiten und beantworten will und deshalb die Speicherung und Bearbeitung aus seinem privaten Bereich vergibt, hat den geschützten Platz des Privaten aufgegeben und keinen Anspruch auf einen besonderen Schutz für die individuelle Privatsphäre durch die Verfassung.

4) **orts- und grenzunabhängige Beweissicherung**
Die Täter wissen ganz genau, in welche Serversysteme sie hacken müssen. Die am meisten unbeobachteten Server stehen in Südostasien und werden entsprechend missbraucht. Die USA und Brasilien stehen dem nicht nach. Das System der Rechtshilfe muss deshalb im Zusammenhang mit der Internetkriminalität ganz neu auf schnelle und direkte, besonders auch (staatlich) einseitige Anordnungen ausgerichtet werden, weil immer wieder Sofortmaßnahmen erforderlich sind.

   Notwendig sind nicht autoritärstaatliche Beweisführungen, sondern schlichte Beweismittelerhebungen, über deren inhaltliche Verwertung durchaus erst im Zwischen- oder Hauptverfahren entschieden werden kann. Schnelle Entscheidungen der Strafverfolgunsbehörden dienen vielfach nicht nur der Überführung von Tätern, sondern der Rettung von Opfern und der Sicherung von Vermögenswerten vor ihrem Entzug in nicht justizförmliche Orte (Karibik?, Baltikum? Südostasien?).

5) **Organisierte Kriminalität**
Die OK ist längst im Internet präsent. Phishing, Botnetze, verteilte Angriffe und die Angebote krimineller Hilfsleistungen sind bekannt und von Deutschland aus nicht allein verfolgbar.

Ineffektive Strafverfolgung

Die materiellen und formellen Instrumente zur Verfolgung der Cybercrime sind unvollständig

Um Tat- und Täterstrukturen im Zusammenhang mit dem Einsatz technischer Mittel aufzuklären, bedarf es adäquater Ermittlungs- und Sicherungsmethoden.

Strafverfahrensrecht

Der Gesetzgeber hat bereits damit reagiert, dass er die klassische Telefonüberwachung auf elektronische Daten erweitert (Überwachung der Telekommunikation, § 100a StPO), den IMSI-Catcher eingeführt (§ 100i StPO), die Auskunft über Verkehrsdaten (§ 100g StPO) und die Wohnraumüberwachung geregelt hat (§ 100c StPO).

Wegen des Datenverkehrs in Netzen fehlt es jedoch noch häufig an klaren Festlegungen. Das gilt sowohl für die Speicherung von Verkehrsdaten (Vorratsdatenspeicherung) wie auch für private Onlinedaten, die von Hostprovidern aufbewahrt werden (E-Mail-Postfächer, Dokumentenspeicher). In diesen Fällen ist die Praxis darauf angewiesen, aus den allgemeinen Vorschriften Eingriffsbefugnisse abzuleiten (Beschlagnahme körperlicher Datenträger gemäß § 94 StPO, Überwachung der Telekommunikation gemäß § 100a StPO) oder Analogien zu bilden, z.B. zur Postbeschlagnahme gemäß § 99 StPO im Zusammenhang mit der Sicherung von E-Mails. Auch dort, wo der Gesetzgeber bereits gehandelt hat, hinterließ er Lücken, die von der Praxis und der Rechtsprechung schwerfällig geschlossen werden mussten, z.B. im Zusammenhang mit dynamischen IP-Adressen. Noch heute besteht Streit darüber, ob sie Bestandsdaten gemäß § 113 Telekommunikationsgesetz – TKG – oder Verkehrsdaten gemäß § 100g StPO sind.

An einer Pflicht zur aktiven Mitwirkung unbeteiligter Dritter wie Banken und Provider fehlt es ebenfalls (Editionspflicht), so dass gefilterte und zusammenhängende Auskünfte über Kontobewegungen oder Telekommunikationsverbindungen nur im Wege der Abwendungsbefugnis zur Vermeidung schwe-

rerer hoheitlicher Maßnahmen durchgesetzt werden können [13].

Vielfach haben die Vorgaben des Gesetzgebers eher zu Arbeitsbeschaffungen für die Staatsanwaltschaften geführt. So wird ein Auskunftsanspruch privater (und gewerblicher) Geschädigter gegen den Zugangsprovider des Störers (zusammen mit einer Begrenzung der Gebührenhöhe für Abmahnungen) erst jetzt eingeführt, nachdem das Bundesjustizministerium in der Vergangenheit immer die Auffassung vertreten hat, die Geschädigten mögen sich zunächst mit einer Strafanzeige an die Staatsanwaltschaft richten, die dann ihrerseits die Auskunft einholt – und die damit verbundenen Kosten trägt.

Mit dem von Deutschland noch nicht eingeführten Cybercrime-Abkommen wird der erste Schritt zu einer grenzüberschreitenden Strafverfolgung unternommen, die bislang häufig an langwierigen und aufwändigen Rechtshilfeverfahren scheitert.

Strafrecht

Auch wegen der materiellen Strafvorschriften hat der Gesetzgeber bislang nur mäßig reagiert. Der Entwurf der Bundesregierung für das Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität [14] aus dem September 2006 sieht erstmals

1. die Strafbarkeit des reinen Eindringens in EDV-Systeme (Hacking, § 202a StGB),
2. den Schutz privater Datenverarbeitungen vor Sabotage (§ 303b StGB) und vor verteilten Angriffen (DoS-Attacken),
3. die Strafbarkeit des Abhörens von elektromagnetischer Abstrahlung (§ 202b StGB) und
4. des Herstellens, Überlassens, Verbreitens oder Verschaffens von „Hacker-Tools“ vor.

Wegen der Strafbarkeit von Hacker-Tools sind die praktischen Probleme bereits vorbestimmt:

§ 69e Urhebergesetz erlaubt dem Lizenznehmer ausdrücklich die Dekompilierung von Computerprogrammen zur Herstellung ihrer Interoperabilität. Dabei muss der maschinensprachliche Programmcode in logische, menschenverständliche Kommandos und Routinen zurückverwandelt werden. Ohne Programme, die auch zum rechtswidrigen Cracking verwendet werden können, ist das nicht möglich.

Die Verwaltung, Beobachtung und Sicherung von Computernetzwerken macht den Einsatz von automatischen Analysekommandos und -programmen nötig, die von einfachen Verbindungsprüfungen (Ping, Tracerouting) über die Ausfallsicherheit (Monitoring) und die Lastverteilung (Load Balancing) bis hin zur Abwehr von Angriffen aus dem Netz reichen (Intrusion Detection). Alle dazu eingesetzten Programme lassen sich auch rechtswidrig missbrauchen und sind prinzipiell Hacker-Tools.

Wegen der Massenplagen der unerwünschten Werbe-E-Mails (Spamming), der Malwareträger (Würmer, Trojaner mit Schadensfunktionen) und der Aufforderung zur Preisgabe privater Vermögensdaten (Phishing) muss die Strafverfolgung die „Fälschung beweiserheblicher Daten“ (§ 269 StGB) bemühen, die aber die E-Mails zur Anwerbung von Finanzagenten nur dann erfasst, wenn sie falsche Absenderangaben enthalten.

Wegen ihrer Auswirkungen schlimmer und gefährlicher als individuelle Hackerangriffe sind Botnetze mit Tausenden ferngesteuerter PCs, die sich zum massenhaften Versand von E-Mails, zu verteilten Angriffen oder zur Verschleierung krimineller Einzelaktionen missbrauchen lassen. Zu ihrer Überwachung und Steuerung kommen Programme zum Einsatz, die nichts mit „Hacker-Tools“ gemein haben, sondern deren Funktionsprinzipien aus der Netz- und Systemüberwachung stammen. Im Gegensatz zu den „guten“ Programmen zur Softwareverteilung, zur Fernüberwachung (Remote) oder zur Fernsteuerung werden sie mit Malware verteilt und wirken ohne das Wissen und Wollen des betroffenen PC-Besitzers.

Zur Abwehr von Botnetzen, von Spam- und Phishingkampagnen wären (international gleiche) Gefährdungstatbestände wünschenswert, die z.B. die Transparenz von Programmfunktionen zum Ziel erheben und versteckte Funktionen außerhalb der Kontrolle des Anwenders unter Strafe stellen.

---

13 Die Abwendungsbefugnis richtet sich in aller Regel gegen die Duldung einer polizeilichen Durchsuchung beim unbeteiligten Dritten (§ 103 StPO) und einer anschließenden Beschlagnahme (§ 94 StPO). „Kontoverdichtungen“ können als Schriftstücke in der Hauptverhandlung verlesen werden (§ 249 StPO). Ihre inhaltliche Richtigkeit muss hingegen durch einen Zeugenbeweis eingeführt werden.

14 Pressemitteilung des BMJ vom 20.09.2006.

Einen intelligenten Schritt in diese Richtung hat der Gesetzgeber 2003 mit dem Gesetz gegen den Missbrauch von Mehrwertdiensten unternommen, indem er eine Registrierungspflicht für Mehrwertdienstenummern (0190 [ausgelaufener Nummernkreis], 0900) und für Einwahlprogramme (Dialer) eingeführt hat. Die Anbieter, die nicht in den Datenbanken der Bundesnetzagentur aufgeführt oder aus ihnen wieder gelöscht sind, können ihre (vorgeblichen) Forderungen nicht mehr im Zivilrechtsweg durchsetzen. Seither gibt es kaum noch Dialer und ihre kriminellen Varianten sind fast vollständig vom Markt verschwunden.

Ahnungslosigkeit

Politik, Rechtspflege und Strafverfolgung können auf die aktuellen Formen der IuK-Kriminalität nicht angemessen reagieren, weil

1. das Personal zur Rechtsanwendung fehlt,
2. dem vorhandenen Personal das erforderliche Wissen fehlt und
3. es an einer systematischen Analyse der Bedrohungspotentiale, Tendenzen und Strukturen fehlt.

Das Bundeskriminalamt hat sich im Zusammenhang mit seiner anlassunabhängigen Internetrecherche die Analyse von Phishing-Kampagnen zu eines seiner Arbeitsschwerpunkte gesetzt. Ohne die Beteiligung der juristischen Strafverfolgungspraxis und von Hochschulen kann seine Arbeit aber nur ein unvollständiges Bild ergeben. Hilfreich wäre eine internationale Einrichtung, die die Erfahrungen der Polizei, der Justiz und aus der Wissenschaft bündelt und Empfehlungen entwickelt, wie den aktuellen Kriminalitätsformen entgegen gewirkt werden kann.