erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Klaus-Peter Löhr

Der Staat hackt mit

Mehr Sicherheit durch Bundestrojaner?

„Die meisten Menschen sind über Terrorismus und Kriminalität beunruhigt, nicht über polizeiliche Schutzmaßnahmen. Sie wollen, dass der Staat ihre Sicherheit garantiert. Dazu muss er auch neue Technologien nutzen. Wir können nicht stehen bleiben, wenn das Verbrechen und der Terrorismus immer neue Kommunikationsmöglichkeiten zur Verfügung haben."

... so Innenminister Dr. Schäuble im Interview mit der *taz* vom 8.2.07. Zum Bündel der einschlägigen Initiativen des Innenministeriums (BMI) und des ihm unterstellten Bundeskriminalamts (BKA) gehört die sogenannte *verdeckte Online-Durchsuchung* der Rechner von Personen, die der Vorbereitung oder Durchführung von Straftaten verdächtigt werden, zu Zwecken der Prävention oder Strafverfolgung. Verdeckte Online-Durchsuchung bedeutet, dass Polizei oder Strafverfolgungsbehörden sich über das Internet unbemerkt Zugang zum Rechner eines Verdächtigen verschaffen und dort Software installieren, mit der gespeicherte Daten ausgelesen werden können. Auch eine längerfristige Überwachung des Verhaltens des Benutzers ist auf diese Weise möglich.

Technische Grundlage: IT-Unsicherheit

Das unbefugte und unbeobachtete Eindringen in fremde Rechner über das Netz wird überhaupt erst dadurch möglich, dass die meisten Systeme nur unzureichend gegen solche Angriffe geschützt sind, bedingt durch Software-Mängel oder durch Nachlässigkeit der Benutzer. Der Einbruch in einen Rechner über das Netz ist insofern mit dem Einbruch in eine Wohnung zu vergleichen, die entweder ein schlechtes Schloss hat oder nicht richtig abgeschlossen ist.

Besonders problematisch ist, dass gerade populäre, weit verbreitete Systeme eine Vielzahl von Schwachstellen aufweisen, die von gewieften Hackern für erfolgreiche Angriffe ausgenutzt werden können. Da solche Angriffe schwerwiegende Folgen haben können – von Datenspionage bis hin zur Sabotage – sind sie natürlich strafbar. Erst kürzlich wurde mit der Erweiterung des § 202 Strafgesetzbuch (StGB) sogar die Entwicklung entsprechender Werkzeuge unter Strafe gestellt. (Siehe dazu die Presseerklärung des FIfF vom 16.7.2007.)

Zu beobachten ist andererseits, dass sich die Software-Entwickler zunehmend der Verantwortung für die Qualität ihrer Produkte bewusst werden. In der Informatik hat das Thema *IT-Sicherheit* endlich den gebührenden Stellenwert erhalten. Die Zukunftsvision sind sichere Systeme, die das gesetzliche Verbot der *Überwindung der Zugangssicherung* (§ 202a(1) StGB) entbehrlich machen würden – weil nämlich ihre Zugangssicherung unüberwindbar ist. Man kann darüber streiten, wie realistisch eine solche Vision ist; unstrittig ist, dass schon heute viel getan werden kann, um die Sicherheit unserer Systeme deutlich zu er-

höhen. Damit würden womöglich auch die Initiativen für eine verdeckte Online-Durchsuchung ins Leere laufen; wir kommen später darauf zurück.

Was genau ist der *Bundestrojaner*?

Die vielen Schwachstellen in heutigen IT-Systemen sind von sehr unterschiedlicher Art, und dementsprechend gibt es eine Vielzahl unterschiedlicher Einbruchstechniken. Gemeinsam ist ihnen, dass der Angreifer versucht, *Schadsoftware* mit verdeckter Funktionalität auf dem Rechner zu installieren, die mehr oder weniger gravierende Auswirkungen haben kann (und im Übrigen auch als Basis für weitere Angriffe im Netz dienen kann). Eine grobe Klassifikation orientiert sich daran, ob ein spezifisches Benutzerverhalten die Voraussetzung für einen erfolgreichen Angriff darstellt, oder ob der Angreifer auch bei völliger Inaktivität des Benutzers Erfolg haben kann.

Letzteres ist bei einem nicht bereits mit Schadsoftware infizierten Rechner schwierig bis unmöglich (abhängig von der Sorgfalt, mit der der Eigentümer die vorgesehenen Schutzmechanismen einsetzt – wie etwa eine Firewall). Daher sind Angriffe beliebt, die auf die Unachtsamkeit des Benutzers im täglichen Umgang mit dem Rechner setzen. Jede Aktion des Benutzers, die einen Datenfluss aus dem Netz in den eigenen Rechner zur Folge hat, ist ein potenzielles Einfallstor für Schadsoftware.

Dieser Sachverhalt ist offensichtlich, wenn ich etwa ein attraktiv erscheinendes Programm aus dem World-Wide-Web herunterlade. Denn eigentlich müsste ich mir vorher die folgenden Fragen stellen – und beantworten: Worauf gründe ich mein Vertrauen, dass dieses Programm genau das tut (nicht mehr und nicht weniger), was mir versprochen wurde? Wenn es von Microsoft oder von XYZ kommt, vertraue ich Microsoft bzw. XYZ? Wenn ich es über eine Webseite beziehe, auf der Microsoft steht, worauf gründe ich mein Vertrauen, dass wirklich Microsoft für diese Seite verantwortlich ist?

Die meisten Menschen stellen sich diese Fragen nicht, mit dem Effekt, dass ihnen leicht etwas untergeschoben werden kann, was sie gar nicht haben wollten. Wenn sie das bei der Benutzung des Programms merken, ist es vielleicht schon zu spät, und das Programm kann bereits beträchtlichen Schaden angerichtet haben.

Tückischer sind Programme, die durchaus die versprochene Leistung erbringen, daneben aber noch eine verborgene, schädliche Funktionalität aufweisen, die lange unentdeckt bleiben kann. Ein solches Programm wird als Trojanisches Pferd – im Jargon Trojaner – bezeichnet.

Für die verdeckte Online-Durchsuchung sind Trojanische Pferde das ideale Vehikel: mit passender Funktionalität versehen und einmal eingeschleust, können sie alle möglichen Aktivitäten entwickeln, vom Durchsuchen der Festplatte über das Protokollieren von Tastatureingaben (keylogging) bis hin zur Kontaktaufnahme mit anderen Rechnern. Und selbstverständlich können sie in Kontakt mit ihrem Herkunftsort bleiben, gefundene Daten dorthin übermitteln und ferngesteuert ihr Verhalten verändern. Das geht so weit, dass über sie auch die am Rechner womöglich vorhandenen Mikrofone und Kameras gesteuert werden können (!).

Diese weitreichenden Möglichkeiten erklären, warum der Begriff *Bundestrojaner* mittlerweile zum Synonym für jegliche Schadsoftware für die verdeckte Online-Durchsuchung geworden ist. Zur Präzisierung muss gesagt werden, dass es *den* Bundestrojaner – im Sinne eines *universell* einsetzbaren Werkzeugs – nicht gibt. Für jeden Einzelfall – z.B. einen bestimmten Terrorverdächtigen – muss ein den spezifischen Umständen entsprechender Angriff konzipiert und mit erheblichem Aufwand ein maßgeschneidertes Trojanisches Pferd entwickelt werden. Das liegt an der Vielzahl der existierenden Systeme, ihren verschiedenen Varianten und Versionen, dem unvollständigen Wissen über die Installation bei dem Verdächtigen und nicht zuletzt an den Schwierigkeiten, dem Verdächtigen das Trojanische Pferd tatsächlich unterzuschieben – zumal wenn dieser Vorsicht walten lässt.

Nach einem Bericht der ARD vom 27.4.2007 wurden verdeckte Online-Durchsuchungen vom Bundesnachrichtendienst bereits in mehreren Fällen durchgeführt, und zwar auf der Grundlage einer vom früheren Innenminister Otto Schily erlassenen Dienstvorschrift.

Die Rechtslage

Eine vom Generalbundesanwalt beantragte verdeckte Online-Durchsuchung im Rahmen eines Ermittlungsverfahrens wurde vom Ermittlungsrichter des Bundesgerichtshofs (BGH) am 21.2.06 genehmigt, dann aber (vermutlich wegen technischer Schwierigkeiten) de facto nicht durchgeführt. Die Genehmigung erfolgte mit Bezugnahme auf §§ 105, 106 (Wohnungsdurchsuchung) der Strafprozessordnung (StPO). Ein zweiter Antrag des Generalbundesanwalts (u.a. wegen des Verdachts der Gründung einer terroristischen Vereinigung) wurde von einem anderen Ermittlungsrichter des BGH abgelehnt. Begründet wurde die Ablehnung damit, dass eine verdeckte Online-Durchsuchung einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung darstelle und durch die StPO nicht gedeckt sei, da die typischen Kriterien für eine Wohnungsdurchsuchung nicht erfüllt seien. Die gegen diese Entscheidung eingelegte Beschwerde des Generalbundesanwalts wurde vom 3. Strafsenat des BGH am 31.1.07 verworfen. Somit bleibt der Bundestrojaner bis zur Schaffung einer gesetzlichen Grundlage illegal.

Der Innenminister hat mittlerweile wiederholt deutlich gemacht, dass er den Bundestrojaner für unverzichtbar hält und daher in Abstimmung mit dem Justizministerium eine entsprechende Gesetzesinitiative auf den Weg bringen will. Vielfach wird bezweifelt, ob ein solches Gesetz vor dem Bundesverfassungsgericht Bestand hätte. Der Innenminister scheint entschlossen, wenn erforderlich auch eine Änderung des Grundgesetzes (Art. 13) anzustreben.

In diesem Zusammenhang ist auf die Situation in Nordrhein-Westfalen hinzuweisen. Der Landtag hat am 20.12.06 mit den Stimmen der Regierungskoalition (CDU und FDP) ein Gesetz verabschiedet, das einen Landestrojaner erlaubt: Der Verfassungsschutz des Landes Nordrhein-Westfalen darf unter bestimmten Bedingungen verdeckte Online-Durchsuchungen durchführen. Gegen dieses Gesetz sind zwei Verfassungsbeschwerden beim Bundesverfassungsgericht anhängig; eine Entscheidung wird für Anfang 2008 erwartet.

Sollte der Bundestrojaner legalisiert werden ...

... sind dann die an ihn geknüpften Hoffnungen von Polizei, Strafverfolgern und Verfassungsschützern überhaupt realistisch? Weiter oben wurde bereits darauf hingewiesen, dass das gezielte Installieren eines Trojanischen Pferdes keine einfache Sache ist. Kriminelle Organisationen verfügen heute über genügend informatische Kompetenz, um die Gefährdung ihrer Systeme durch Schadsoftware gut einschätzen zu können und sich entsprechend vorsichtig zu verhalten. Man kann davon ausgehen, dass ihre Systeme einen höheren Sicherheitsstandard aufweisen als die des Normalbürgers. Ein halbwegs intelligenter Terrorist wird vorsichtig genug sein, kein unbekanntes Programm aus dem Netz herunterzuladen. Wie können BKA-Ermittler trotzdem erfolgreich sein?

Am Beispiel der Viren, die einen Rechner befallen können, kann man sehen, dass man sich Schadsoftware auch ohne das bewusste Herunterladen von Programmen einfangen kann. Viele Benutzer wissen heute, dass man eine Anlage – z.B. ein Textdokument – zu einer E-Mail zweifelhafter Herkunft besser nicht öffnen sollte. Das Tückische bei dieser Art des Angriffs ist, dass man in einem Textdokument kein Programm vermutet. Dennoch kann ausführbarer Code in ihm verborgen sein, der durch das Öffnen des Dokuments aktiviert wird. Dieser Code realisiert typischerweise Makrobefehle zur Texteditierung und ist somit eine nützliche Sache. Er kann aber eben auch schädliche Funktionalität beinhalten. Traditionell ist das die Infektion des Rechners mit einem Virus, der sich über das Netz (z.B. wiederum über E-Mail) weiter verbreitet. Das BKA könnte diese Technik einsetzen, um Schadsoftware im Rechner eines Verdächtigen zu installieren; technisch läge in diesem Fall kein Virus vor (weil keine Weiterverbreitung), sondern eine Art Trojanisches Pferd. Allerdings ist es schwer vorstellbar, dass der intelligente Terrorist auf diesen wohlbekannten Trick hereinfällt – womöglich noch unter Ignorierung einer Warnung, die er vom Viren-Scanner beim Versuch erhält, die E-Mail-Anlage zu öffnen.

Für das Unterschieben von Schadsoftware gibt es aber noch raffiniertere Methoden. Auch beim Umherwandern im Web, also beim Betrachten von Webseiten mit Endungen .html oder .htm (die ja schließlich keine Programme sind) kann man sich Schadsoftware einfangen. Auch in Webseiten kann Programmcode eingebettet sein, sogar in noch viel flexiblerer Weise als man das von Textdokumenten her kennt. Diese Technik dient auch hier einem guten Zweck, ermöglicht sie doch interaktive Webseiten, die man nicht nur passiv betrachten kann. Den auch hier möglichen Missbrauch versucht man dadurch zu verhindern, dass der Browser, unter dessen Kontrolle der Code läuft, diesem Code ein nur sehr eingeschränktes Agieren erlaubt und somit schädliche Aktionen verhindert. Soweit die Theorie. Leider gibt es aber, wie in jeder komplexen Software, auch bei Browsern Schwachstellen, die einem raffinierten Angreifer ein Umgehen der Schutzfunktionen erlauben. Somit kann eine harmlos aussehende Webseite Code im Gepäck führen, der eine schädliche Wirkung entfaltet, ohne dass der Benutzer es merkt. Auch Webseiten können also wie Trojanische Pferde wirken.

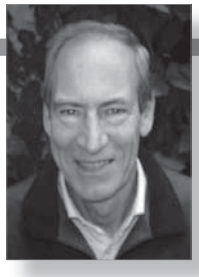
Der schädliche Code muss nicht einmal direkt in der präparierten Seite enthalten sein (bzw. vom Server der Seite nachgeladen werden). Eine spezielle Direktive in einer Seite (das *<iframe> tag*) ermöglicht das Einbetten einer beliebigen anderen Seite – aus beliebiger Quelle – in einen Teilbereich der angezeigten Seite. Damit kann eine Seite so präpariert werden, dass beim Laden zusätzlich eine ganz andere Seite geladen wird, *und zwar unbemerkt,* denn für die Größe des Teilbereichs kann der Wert 0 eingestellt werden. Der Browser wendet sich dann nach dem Laden der ersten Seite an den Server des Angreifers, und von dort wird die Schadsoftware geladen, ohne dass der Benutzer es merkt.

Diese Technik kann dahingehend verfeinert werden, dass der Server des Angreifers, wenn er vom Browser des Opfers kontaktiert wird, Details über dessen Betriebssystem und den Browser abfragen kann. Mit diesem Wissen kann er, wenn er einen Fundus von Schadsoftware-Varianten für verschiedene Systeme vorhält, daraus die für das Opfer passende Variante wählen. Diese Idee wurde jüngst von einem russischen Hacker-Team umgesetzt und unter dem Namen *Mpack* auf den (kommerziellen!) Markt gebracht.

Treffen Sie irgendwelche Vorsichtsmaßnahmen, bevor Sie eine Webseite in Ihren Rechner holen? Sehen Sie sich die URL eines Links in der Fußzeile an, bevor Sie auf das Link klicken? Wenn ja, wie entscheiden Sie, ob sich dahinter eine vertrauenswürdige Webseite verbirgt? Vielleicht war die Seite ursprünglich vertrauenswürdig, ist aber inzwischen durch einen Hacker mit einer Schadfunktion versehen worden. Wenn die Seite über das https-Protokoll angesprochen wird, wiegen Sie sich dann in Sicherheit und klicken? Sie könnten anschließend – wenn Sie sehr sorgfältig sind – das Zertifikat des Webservers prüfen; der Schaden wäre dann aber schon eingetreten. Und auch ein einwandfreies Zertifikat garantiert nicht die Abwesenheit einer verborgenen unerwünschten Funktionalität.

All dies kommt dem verdeckten BKA-Ermittler entgegen (besonders so etwas wie *Mpack*). Wenn wir davon ausgehen, dass der vom Ermittler ins Visier genommene Terrorverdächtige beim Herumwandern im Web keine extreme Vorsicht walten lässt, muss der Ermittler nur noch dafür sorgen, dass der Verdächtige eine von ihm geeignet präparierte Webseite besucht.

Klaus-Peter Löhr



Prof. Dr.-Ing. Klaus-Peter Löhr ist Professor für Informatik a.D. an der Freien Universität Berlin, Fachbereich Mathematik und Informatik. Seine Fachgebiete sind Systemsoftware, Softwaretechnik und IT-Sicherheit. Er ist Mitglied des Präsidiumsarbeitskreises *Datenschutz und IT-Sicherheit* der Gesellschaft für Informatik.

Das ist allerdings leichter gesagt als getan und erfordert einiges *social engineering*. Die Kooperation mit den Betreibern beliebter Webserver – oder jedenfalls solcher, deren Seiten der Verdächtige vermutlich häufiger besucht – ist hilfreich; dort könnten dann eine präparierte Seite sowie dorthin verweisende *attraktive* Links auf anderen Seiten untergebracht werden. Spielt der Betreiber nicht mit, könnte der Ermittler versuchen, die Seiten heimlich entsprechend zu manipulieren (falls das vom Gesetz gedeckt wäre ...).

Das Ganze scheitert natürlich, wenn der Verdächtige das Herumwandern im Web vermeidet oder dafür einen anderen Rechner verwendet als den, auf dem seine sensiblen Daten liegen. Die professionell organisierte Kriminalität wird ohnehin ihre Systeme so organisieren, wie man das von sicherheitsbewussten Unternehmen kennt – mit mehrstufigen Firewalls zwischen Internet und Intranet, *entmilitarisierten Zonen*, sorgfältig nach Funktionalität getrennten Rechnern etc. Zu den weiteren Techniken, mit denen man den Ermittlern das Leben schwer machen kann, gehört natürlich auch die Verschlüsselung der Datenbestände. Die Durchsuchungssoftware muss dann über eine *Keylogging*-Funktionalität verfügen, die den Benutzer bei der Eingabe einer Passphrase für einen Schlüssel erwischt.

Der oben skizzierte Angriff auf einen Rechner ist nicht der einzig mögliche. Es können hier weder alle denkbaren Angriffe noch alle denkbaren Abwehrmechanismen gegen die verdeckte Online-Durchsuchung und auch nicht alle denkbaren Verfeinerungen und Erweiterungen des Bundestrojaners diskutiert werden. Die Liste der Möglichkeiten ist unbegrenzt – wie ja auch im täglichen Geschäft der Kampf zwischen dem IT-Sicherheitsexperten und dem Hacker dem Wettlauf zwischen Hase und Igel gleicht. Festzuhalten ist, dass die verdeckte Online-Durchsuchung einerseits technisch machbar ist (jedenfalls solange unsere Systeme Qualitätsmängel haben), andererseits aber trotz aller Automatisierungsmöglichkeiten ein schwieriges Unterfangen bleibt. Es ist wenig wahrscheinlich, dass der Bundestrojaner – so er denn kommt – bei ausgebufften Kriminellen erfolgreich einsetzbar sein wird.

Außer den beschriebenen gibt es noch zwei (vielleicht auch mehr) andere Ansätze für eine verdeckte Online-Durchsuchung. Erstens: der Staat könnte in die Infrastruktur des Internet eingreifen; ein Erfolg wäre angesichts der supranationalen Struktur des Internet allerdings zweifelhaft. Zweitens: der Rechner eines Verdächtigen könnte in dessen Wohnung direkt manipuliert werden (vergleichbar dem Verwanzen einer Wohnung). – Auch für derartige Ansätze existiert gegenwärtig keine Rechtsgrundlage.

Quo vadis, IT-Sicherheit?

Dass die Datenschutzbeauftragten, die Opposition im Bundestag, das FIfF, die Humanistische Union, der Chaos Computer Club etc. eine Legalisierung der verdeckten Online-Durchsuchung ablehnen, überrascht nicht; handelt es sich doch um einen weiteren Eingriff in Grundrechte (Unverletzlichkeit der Wohnung, informationelle Selbstbestimmung), einen Eingriff, dessen Verhältnismäßigkeit angesichts der nur mäßigen Erfolgsaussichten im Kampf gegen Schwerstkriminalität zweifelhaft erscheint. Die Position der Gegner wird bisweilen pointiert zusammengefasst durch den Satz „Die Regierung unterstützt die Terroristen bei der Abschaffung des liberalen Rechtsstaats". Auch die Medien zeigen sich weitgehend skeptisch bis ablehnend gegenüber den Plänen des Innenministers.

Bemerkenswert ist, dass auch informatische Fachverbände – die auf politische Neutralität achten – die Pläne dezidiert ablehnen. So hat sich die Gesellschaft für Informatik e.V. am 12.7.07 gegen eine Änderung des Art. 13 GG mit dem Ziel der Legalisierung des Bundestrojaners ausgesprochen. Nach einer Pressemeldung des IT-Unternehmensverbands Bitkom vom 23.4.07 lehnt auch die deutsche IT-Wirtschaft den Bundestrojaner ab. Die Fachverbände fürchten einerseits eine Schwächung von Bürgerrechten und Datenschutz (auch Schutz von Firmendaten) und andererseits bei IT-Sicherheitsprodukten Nachteile im internationalen Wettbewerb, die sich ergeben könnten, wenn es politischen Druck gegen zu viel IT-Sicherheit – weil nachteilig für die Ermittler – gibt.

Hier zeigt sich schlaglichtartig das Bizarre an der Diskussion um den Bundestrojaner. Wir alle wissen: IT-Systeme sind unsicher, erst recht im Netz. Dieser Mangel ist nicht naturgegeben, sondern menschengemacht. Die einschlägigen Unternehmen bekennen sich zu ihrer Verantwortung und versprechen Besserung. Wissenschaft und Technik arbeiten an sicheren Systemen. Etliche Unternehmen unterstützen die Initiative *Deutschland sicher im Netz e.V.,* die verkündet: „Der Verein wird die Zielgruppen, Hersteller und Betreiber ... informieren und sensibilisieren, aufklären und beraten sowie neue Schutzmaßnahmen identifizieren und etablieren, um die Sicherheit und das Vertrauen in das Internet und die Informationstechnologie zu stärken." Diese Initiative wird von der Regierung unterstützt. Der Innenminister, der für die Umsetzung des 2005 beschlossenen *Nationalen Plans zum Schutz der Informationsinfrastrukturen* zuständig ist, verkündete am 19.6.07: „Der Verein ‚Deutschland sicher im Netz e.V.' bündelt wichtige gesellschaftliche Akteure zum Thema IT- und Internet-Sicherheit und wird zukünftig ein bedeutsamer Partner für die Politik und alle gesellschaftlichen Gruppen sein. Deshalb werde ich die Arbeit des Vereins als Schirmherr gerne unterstützen".

Möchte der Minister nun nach Kräften die *IT-Sicherheit* befördern oder will er den Bundestrojaner, d.h. *IT-Unsicherheit*? Beides zu wollen, birgt die Gefahr der Schizophrenie. Zumindest stünde der Minister, wenn er seine Schirmherrschaft für *Deutschland sicher im Netz* ernst nimmt, in einem Zielkonflikt. Man tut ihm wohl nicht unrecht mit der Feststellung, dass er verdeckte Online-Durchsuchungen für wichtiger hält als die IT-Sicherheit. Das wirft im übrigen auch ein ungünstiges Licht auf das ihm unterstellte *Bundesamt für Sicherheit in der Informationstechnik* (BSI), das eigentlich bestrebt sein müsste, die Sicherheitslücken zu bekämpfen, die der Bundestrojaner ausnutzen soll.

Man könnte allerdings auch sagen, dass Herr Schäuble mit seinem Kampf um Troja, ob legalisiert oder nicht, den Kampf für mehr IT-Sicherheit jetzt schon erfreulich befördert hat. Die Informatik wird ihr Engagement gegen Schadsoftware verstärken, unabhängig davon, ob sie von Kriminellen oder vom BMI stammt. Ironischerweise ist in diesem Sinn die eingangs gestellte Frage „Mehr Sicherheit durch Bundestrojaner?" durchaus positiv zu beantworten.

Hilfreich für weitere Recherchen (Stand: 15.10.2007):

Wikipedia gibt einen knappen Überblick über die Materie, mit etlichen guten Verweisen: http://de.wikipedia.org/wiki/Bundestrojaner

Es gibt eine eigene Website zum Bundestrojaner: unter *http://www.bundestrojaner.de/* findet man aktuelle Nachrichten, ein Archiv, Stellungnahmen, Abwehrmaßnahmen und weiteres.

Sehr empfehlenswert – weil reich an Informationen, präzise und gut lesbar – ist der Aufsatz von Ulf Buermeyer, Die „Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, in HRRS: *http://www.hrr-strafrecht.de/hrr/archiv/07-04/index.php?sz=8*

Zum selben Thema siehe Hartmut Pohl, Zur Technik der heimlichen Online-Durchsuchung, in DuD – Datenschutz und Datensicherheit 31 (2007) 9, *http://www.dud.de/index.php;sid=b9be118ba4ddd5346739103ffa7e89cd/site=dud/do=show/id=471/alloc=122*

Dem juristisch interessierten Leser sei das Studium der BGH-Entscheidung vom 31.1.07 empfohlen: *http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=2007&Sort=3&Seite=9&nr=38779&pos=277&anz=514*

Der technisch interessierte Leser möchte sich vielleicht genauer über Mpack informieren:

http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html

http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf?sitepanda=particulares

erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

'society [is] willing to recognize that expectation as reasonable.'"

The Court concluded that viewing the home with a thermal imager was a search requiring a warrant:

> *"Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."*

The 6th Circuit applied the same analysis to email in Warshak. It had to find both a subjective expectation of privacy … and that … "society [is] willing to recognize that expectation as reasonable.

The court drew analogies, to telephone calls and the mail. In both cases long precedents define and protect the contents of mail and the telephone call:

> *"Two amici curiae convincingly analogize the privacy interest that e-mail users hold in the content of their e-mails to the privacy interest in the content of telephone calls, … because the caller 'is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,' and therefore cannot be said to have forfeited his privacy right in the conversation"*

However in both telephone calls and mail the courts distinguish the protected contents of the transmission from the unprotected address and routing information.

> *"although the conduct of the telephone user in Smith 'may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.' … the use of pen register, installed at the phone company's facility to record the numbers dialed by the telephone user, did not amount to a search. This distinction was due to the fact that 'a pen register differs significantly from the listening device employed in Katz, for pen registers do not acquire the contents of communications.'" (Warshak)*

The court carefully looked at the technology to find the difference between content and routing information. The court found that the government's right to the routing information gave it no right to the contents

> *"the government … cannot, on the other hand, bootstrap an intermediary's limited access to one part of the communication (e.g. the phone number) to allow it access to another part (the content of the conversation)"*

The court determined that a search was unreasonable without a warrant and in a key footnote the court further limited the access provided by a warrant

> *"If the e-mails are seized pursuant to a warrant, the Fourth Amendment's particularity requirement would necessitate that the scope of the search somehow be designed to target e-mails that could reasonably be believed to have some connection to the alleged crime being investigated"*

The court declared the relevant portions of the Stored Communications Act unconstitutional and sent the case back to the lower court.

Unless Warshak is overturned by the Supreme Court it represents a declaration of substantial privacy interests in internet communications. Given the aggressive attempts to erode privacy protection after 9/11 it is a welcome reminder of the fundamental importance of privacy.

Sven Lüders

Weit entfernt von der Normalität

Der Gesetzentwurf der Bundesregierung zur Reform der Telefonüberwachung und anderer verdeckter Ermittlungsmaßnahmen

Seit Jahren steigt die Zahl abgehörter Telefonate in Deutschland kontinuierlich an. Allein im letzten Jahr wurden über 41.000 Anordnungen zur Telefonüberwachung erlassen. Dabei werden jedes Mal hunderte bis tausende Gespräche abgehört. Neben den Anschlussinhabern, gegen die sich die Überwachung richtet, sind auch ihre Gesprächspartner betroffen. Nur die wenigsten erfahren davon und können sich dagegen wehren, also nachträglich die Zulässigkeit dieses Eingriffs in ihre Privatsphäre durch ein Gericht prüfen lassen.

Dabei stellen die bekannten Zahlen zur Überwachung der Telefon- und Internetnutzer nur die Spitze des Eisbergs heimlicher Ermittlungsmethoden dar, mit denen Polizei und Staatsanwaltschaften Straftaten aufklären können. Über die heimliche Beschlagnahmung von Postsendungen, den Einsatz verdeckter Ermittler, das längerfristige Observieren und dergleichen Methoden ist kaum bekannt, wie oft, wie lange und wie erfolgreich sie angewandt werden. Bei jedem heimlichen Ermitteln stellt sich die Frage, ob dies für die Aufklärung der jeweiligen Straftaten wirklich angemessen und notwendig war.[1]

Insofern mag man sich über den Gesetzentwurf der Bundesjustizministerin freuen, mit dem sie die Telefonüberwachung reformieren und die verdeckten Ermittlungsmaßnahmen harmonisieren will (BT-Drs. 16/5846). Die Telefone würden künftig nur noch zur Verfolgung schwerer Straftaten überwacht, die