



Vorratsdatenspeicherung / allgemeine Überwachung

MAUS - 16.11.2006 um 14:16

[B]Meldung vom 15.11.2006 12:13

Vorratsdatenspeicherung soll auch für Anonymisierungsdienste gelten[/B]

Der jetzt komplett verfügbare Referentenentwurf zur Neuregelung der Telekommunikationsüberwachung, den Bundesjustizministerin Brigitte Zypries vergangene Woche in Grundzügen vorgestellt hat, bittet deutsche Betreiber von Anonymisierungsservern zum umfassenden Datenprotokoll. Auch "wer einen Anonymisierungsdienst betreibt und hierbei die Ausgangskennung des Telekommunikationsnutzers durch eine andere ersetzt", betreibt einen Telekommunikationsdienst für die Öffentlichkeit und unterliege damit den gleichzeitig vorgeschlagenen Verpflichtungen zur verdachtsunabhängigen Speicherung von Verbindungsdaten für sechs Monate, heißt es in dem Papier (PDF-Datei), das die Humanistische Union online gestellt hat.

Für den Arbeitskreis Vorratsdatenspeicherung und sieben weitere Bürgerrechtsorganisation sind die Pläne ein weiteres Anzeichen dafür, dass die von Zypries vorangetriebene "Totalspeicherung der Telekommunikation der gesamten Bevölkerung vollkommen unverhältnismäßig" sei. Mit einer Videobotschaft an Bundeskanzlerin Angela Merkel, die auf einer Demonstration gegen den Überwachungsstaat in Bielefeld entstand, fordern sie einen Stopp der Umsetzung der EU-Vorgaben zur Vorratsspeicherung von Kommunikationsdaten. Zuvor hatten Datenschützer gehofft, dass etwa der vom Unabhängigen Landeszentrum für den Datenschutz Schleswig-Holstein (ULD) mitbetriebebene Anonymisierungsdienst AN.ON als Teledienst gefasst und damit von den Verpflichtungen zur Datenjagd unberührt bleiben würde. Sie verwiesen darauf, dass sich in Verdachtsfällen der Verkehr von bestimmten IP-Adressen durch die Betreiber der AN.ON-Mixe bereits im Stil des "Quick Freeze"-Verfahrens aufbewahren lasse, bei dem Verbindungsdaten für einen aktuellen Anlass auf Zuruf der Strafverfolger archiviert werden.

Wie aus der Begründung des Referentenentwurfs hervorgeht, hält das Justizministerium das "Einfrieren" von Kommunikationsdaten generell für unzureichend. Es gehe "notwendig ins Leere", wenn die erwünschten "Verkehrsdaten" vom Diensteanbieter "überhaupt nicht gespeichert oder zwischenzeitlich bereits gelöscht wurden". Dies sei aufgrund der Verbreitung von Pauschaltarifen, bei denen Provider Verbindungsdaten für Abrechnungszwecke nicht benötigen und diese daher nach geltendem Recht nicht speichern dürfen, immer häufiger der Fall. Der Entwurf räumt zwar ein, dass "Verkehrsdaten einen besonders schutzwürdigen Aussagegehalt haben, da sie im Einzelfall erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten" der Nutzer zulassen würden. "Hinzu kommt, dass die Datenspeicherung unabhängig von einem im Einzelfall bestehenden Tatverdacht erfolgt und eine unbestimmte Vielzahl von Personen erfasst". Trotzdem überwiege das öffentliche Interesse "der Gewährleistung einer wirksamen Strafverfolgung". Zur Erfüllung dieses Auftrags leiste die gesicherte Verfügbarkeit der umfassenden Nutzerspuren für die Ermittler einen "wichtigen", in einigen Deliktsbereichen wie der Aufklärung komplexer Täterstrukturen und bei "mittels Telekommunikation begangenen Straftaten" gar "unverzichtbaren Beitrag".

Insgesamt geht das Justizministerium davon aus, dass der insgesamt über 200 Seiten starke Entwurf keine Datensammlung "auf Vorrat zu unbestimmten oder noch nicht bestimmbar Zwecken" verlangt und daher mit der verfassungsrechtlichen Rechtsprechung vereinbar ist. Er legt unter anderem fest, dass es für Universitäten oder die Betreiber unternehmensinterner Netze keine Speicherpflicht gibt. Betont wird zudem, dass keine Inhaltsdaten etwa in Form von URLs erfasst werden dürfen. Dies könnte Provider bei der bislang von technischen Protokollen vorgesehenen Verknüpfung von Verbindungs- und Inhaltsdaten bei E-Mail aber in die Bredouille bringen. Überhaupt sieht das Papier in einer Änderung von Paragraph 111 Telekommunikationsgesetz (TKG) vor, dass künftig auch die Anbieter von E-Mail-Konten Kundendaten erheben und ihre Nutzer so eindeutig identifizieren müssen. Die rasche Eröffnung eines Accounts ohne Vorlage eines Personalausweises bei einem deutschen Webmail-Dienst dürfte damit passé sein.

Darüber hinaus öffnet der Entwurf eine Hintertür zur Vorratsdatenspeicherung von erfolglosen oder unbeantwortet bleibenden Anrufen. Dazu wird den Anbietern zunächst etwa freigestellt, Abrechnungsdaten künftig sechs Monate lang vorzuhalten. Mit dem neuen Paragraph 110a TKG mit den Einzelregelungen über die bei der Vorratsdatenspeicherung zu erfassenden Nutzerspuren wird dann aber vorgeschrieben, dass die für diesen Zweck gespeicherten oder generell mitprotokollierten Daten über nicht zustande kommende Anrufe "auch nach Maßgabe dieser Vorschrift" aufbewahrt werden müssen. Dies gelte etwa auch für den Fall, dass ein Mobilfunkanbieter Kunden per SMS über einen Anrufversuch informiere. Bei der Standortdatenabfrage drängt der Entwurf Mobilfunkbetreiber zudem zu möglichst genauen Angaben. So sollen sie bei den zu speichernden Bezeichnungen von Funkzellen auch Daten vorhalten, "aus denen sich

die geografische Lage" der jeweiligen Zelle sowie "die Hauptstrahlrichtung der Funkantennen ergibt".

Nicht ohne Brisanz ist auch die Ausgestaltung des deutlich aufgebohrten Paragraphen 100g Strafprozessordnung (StPO), der die "Erhebung" von Verkehrsdaten durch die Ermittler bei Straftaten regelt – und zwar teilweise in "Echtzeit", wie die Begründung ausführt und dabei etwa auf Auflagen aus der umstrittenen Cybercrime-Konvention des Europarates verweist. Zur Relativierung schlägt das Ministerium hier vor, dass bei der Aufklärung von Delikten von "im Einzelfall erheblicher Bedeutung" eine räumlich und zeitlich "hinreichend bestimmte Bezeichnung der Telekommunikation" genügt, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Bei "mittels Telekommunikation" begangener Straftaten soll die Datenabfrage ferner im Gegensatz zu schwerwiegenderen Fällen nur zulässig sein, wenn die Gesetzeshüter anderweitig nicht vorankommen "und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht". So möchte das Ministerium etwa verhindern, dass Strafverfolger schon bei einer reinen Beleidigung am Telefon auf die Datenhalden zugreifen. Bei zivilrechtlichen Auskunftsansprüchen etwa von Rechthaltern ist ebenfalls keine Datenabfrage vorgesehen. Gemäß Entwurf entfällt aber gleichzeitig die bisher in 100g enthaltene Formulierung, wonach Standortdaten nur "im Falle einer Verbindung" erhoben werden dürfen. Dies mache die umstrittene Übersendung einer "stillen SMS" entbehrlich, da künftig eine Ortung auch dann möglich sei, wenn ein eingeschaltetes Mobiltelefon nicht aktuell genutzt werde.

Für heftige Auseinandersetzungen dürfte letztlich das Vorhaben zählen, der Wirtschaft trotz einer inzwischen eingereichten Verfassungsbeschwerde keine gesonderte Kostenerstattung für die Übernahme der neuen Hilfssheriff-Leistungen zu zahlen. Das Justizministerium geht zunächst sehr vage davon aus, dass die "Anzahl zusätzlicher entschädigungspflichtiger Auskunftersuchen zwischen 500 und 10.000 pro Jahr liegen wird". Dies ergebe nach dem vom JVEG vorgegebenen Stundensatz von maximal 17 Euro pro Auskunftersuchen ein zusätzliches Ausgabevolumen von 8500 bis 170.000 Euro pro Jahr. Den Aufwand der betroffenen Unternehmen für das Beantworten von Verkehrsdatenabfragen will der Entwurf damit abgegolten wissen.

Die "zur Erfüllung der Speicherungspflichten erforderlichen Investitionen" und gegebenenfalls gesteigerten Betriebskosten tut der Entwurf als Peanuts ab. Ein "großer deutscher Diensteanbieter" mit einem Jahresumsatz von annähernd 60 Milliarden Euro habe die Zusatzkosten auf 700.000 Euro pro Jahr beziffert, was 0,00116 Prozent der Einnahmen ausmache. Sollten die Provider diese Aufwendungen auf ihre Kunden "abwälzen" wollen, würde das Verbraucherpreisniveau wohl "allenfalls geringfügig steigen". Der Arbeitskreis Vorratsdatenspeicherung appelliert dagegen dafür, "die über 500 Millionen Euro, welche die geplante Totalprotokollierung Wirtschaft und Staat kosten würde", in ein Programm zur Kriminalitätsprävention vor Ort etwa an Schulen oder einzelnen Stadtteilen zu investieren.

<http://www.heise.de/ct/hintergrund/meldung/81061>
(weiterführende, ergänzende Links im Originaltext)

MAUS - 1.12.2006 um 12:08

[B]30.11.2006 12:37

Arbeitskreis Vorratsdatenspeicherung sieht große Resonanz nach Massenklage-Aufruf [/B]

Eine Woche nach seinem Aufruf zu einer "Sammel-Verfassungsbeschwerde" hat der Arbeitskreis Vorratsdatenspeicherung ein Zwischenfazit gezogen. Mittlerweile haben sich demnach über 6000 Menschen gemeldet, die für den Fall vor das Bundesverfassungsgericht ziehen wollen, dass der Bundestag die von der Koalition geplante Vorratsdatenspeicherung beschließt. Unter den Beschwerdeführern seien viele Journalisten, die um ihre anonymen Informanten fürchteten, teilt der Arbeitskreis mit, sowie Ärzte, Seelsorger, Geistliche, Rechtsanwälte, Unternehmensberater, Suchthelfer und Psychotherapeuten. Beim Berliner Rechtsanwalt Meinhard Starostik, der die Vertretung der Beschwerdeführer vor dem Bundesverfassungsgericht übernimmt, gingen "waschkörbeweise" Vollmachten ein. Anzeige

Der Arbeitskreis hat zudem heute den Bericht "Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten" des Bundeskriminalamts vom November 2005 veröffentlicht (PDF-Datei), von dem bei früher bereits die Rede war. Demzufolge konnten in den vergangenen Jahren 381 Straftaten wegen fehlender Telekommunikationsdaten nicht aufgeklärt werden, vor allem in den Bereichen Internetbetrug, Austausch von Kinderpornografie und Diebstahl. "Die genannten 381 Fälle machen weniger als 0,001 Prozent der 6,4 Millionen jährlich begangenen Straftaten aus", kommentiert Patrick Breyer vom Arbeitskreis Vorratsdatenspeicherung. Angesichts einer Zahl von 2,8 Millionen Delikten jährlich, die meist unaufgeklärt blieben, weil die Täter keine Spuren hinterlassen haben, sei nicht einzusehen, warum gerade die Nutzer von Telefon, Handy und Internet unter Generalverdacht gestellt werden sollten.

<http://www.heise.de/newsticker/meldung/81798>

(weiterführende, ergänzende Links im Originaltext)

MAUS - 1.12.2006 um 13:30

[B]Massenbeschwerde gegen Protokollierung von Telefon, Handy, Mails und Internet

"Totale Bespitzelung geplant"

Von Hildegard Miensopust [/B]

Bürgerrechtler rufen zur Teilnahme an einer "Sammel-Verfassungsbeschwerde" gegen die von der Bundesregierung geplante Protokollierung der Nutzung von Telefon, Handy, Email und Internet auf. Dieser Aufruf zur Erhebung einer Massenverfassungsbeschwerde ist in der deutschen Geschichte einmalig.

[B]Plan der Bundesregierung einzigartig[/B]

"Die von der Bundesregierung geplante Totalprotokollierung der Telekommunikation der gesamten Bevölkerung ist ebenfalls einzigartig", begründet der Politikwissenschaftler Ralf Bendrath vom Arbeitskreis Vorratsdatenspeicherung die Aktion. "Frau Zypries will vorsorglich Informationen über unsere Telefonate, Bewegungen und Internetnutzung sammeln lassen für den Fall, dass wir zu Verbrechern werden. Wir sammeln vorsorglich Beschwerdeführer für den Fall, dass SPD und Union dieses verfassungswidrige Vorhaben tatsächlich umsetzen sollten. Wenn die Koalition unzählige Menschen bespitzeln lassen will, dann werden sich auch unzählige Menschen in Karlsruhe dagegen zur Wehr setzen."

An der vom Arbeitskreis Vorratsdatenspeicherung vorbereiteten Verfassungsbeschwerde kann sich jedermann beteiligen. Auf der Internetseite des Arbeitskreises (www.vorratsdatenspeicherung.de) befindet sich ein Meldeformular. Die Vertretung der Beschwerdeführer vor dem Bundesverfassungsgericht wird der Berliner Rechtsanwalt Meinhard Starostik übernehmen, der Mitglied in dem Verein "RAV - Anwälte/innen für Menschenrechte" ist.

[B]Mit Artikel 10 Grundgesetz - Fernmeldegeheimnis - unvereinbar[/B]

Mit Dr. Rolf Gössner und Prof. Dr. Christoph Gusy unterstützen prominente Erstkläger die Verfassungsbeschwerde. Der Bremer Rechtsanwalt und Bürgerrechtler Rolf Gössner ist Präsident der Internationalen Liga für Menschenrechte (ILMR). Christoph Gusy ist Professor der Rechtswissenschaft an der Universität Bielefeld. Er begründet seine Teilnahme an der Verfassungsbeschwerde wie folgt: "Das geplante Gesetz begründet eine allgemeine, anlassunabhängige Duldungspflicht der Bürger im Hinblick auf mögliche polizeiliche Maßnahmen, welche ohne Wissen des Betroffenen und damit gleichfalls ohne Kontroll- oder Rechtsschutzmöglichkeit durchgeführt werden können. Eine derart allgemeine, breit angelegte Datenerhebung ist mit dem Grundrechtsschutz aus Artikel 10 des Grundgesetzes, dem Fernmeldegeheimnis, unvereinbar."

[B]"Vorsätzlicher Verfassungsbruch"[/B]

"Die anlasslose, zwangsweise Protokollierung der Telekommunikation der gesamten Bevölkerung ist ein eklatanter Verfassungsverstoß", bekräftigt der Jurist Patrick Breyer vom Arbeitskreis Vorratsdatenspeicherung. "Es ist vollkommen unverhältnismäßig, die gesamte Bevölkerung zu erfassen, nur um gegen einige wenige Verdächtige leichter ermitteln zu können. Das Bundesverfassungsgericht hat bereits entschieden, dass 'eine Straftat von erheblicher Bedeutung, ein konkreter Tatverdacht und eine hinreichend sichere Tatsachenbasis' Voraussetzung jeder Erfassung von Verbindungsdaten ist und dass der Gesetzgeber das 'strikte Verbot der Sammlung personenbezogener Daten auf Vorrat' zu beachten hat. Wer gleichwohl das ziellose Anhäufen sensibler Kommunikationsdaten aller Deutschen befürwortet, macht sich des vorsätzlichen Verfassungsbruchs schuldig."

Der Arbeitskreis Vorratsdatenspeicherung fordert, das deutsche Gesetzesvorhaben zumindest solange auszusetzen, bis der Europäische Gerichtshof über die von Irland im Juli eingereichte Nichtigkeitsklage gegen die EG-Richtlinie zur Vorratsdatenspeicherung entschieden hat.

[B]Hintergrund:[/B]

Das Bundesjustizministerium hat vor zwei Wochen einen Gesetzentwurf zur Einführung einer Vorratsdatenspeicherung in Deutschland vorgestellt. Danach soll ab Mitte 2007 zur verbesserten Strafverfolgung über einen Zeitraum von sechs Monaten nachvollziehbar werden, wer mit wem per Telefon, Handy oder Email in Verbindung gestanden hat. Bei Handy-Telefonaten und SMS soll auch der jeweilige Standort des Benutzers festgehalten werden. Anonyme Emailkonten und

Anonymisierungsdienste sollen verboten werden.

Mit Hilfe der gespeicherten Daten können Bewegungsprofile erstellt, geschäftliche Kontakte rekonstruiert und Freundschaftsbeziehungen identifiziert werden. Auch Rückschlüsse auf den Inhalt der Kommunikation, auf persönliche Interessen und die Lebenssituation der Kommunizierenden sind möglich. Die Furcht vor einem Bekanntwerden ihrer Kontakte könnte Informanten, Ratsuchende und Hilfsbedürftige in Zukunft davon abhalten, sich an Journalisten, Anwälte oder Beratungsstellen zu wenden. Der Informantenschutz, das Anwalts- und das Arztgeheimnis würden unterlaufen.

Gegenwärtig dürfen Telekommunikationsanbieter nur die zur Abrechnung erforderlichen Verbindungsdaten speichern. Dazu gehören Standortdaten und Email-Daten nicht. Auch sonstige Verbindungsdaten werden auf Wunsch monatlich gelöscht. Durch die Benutzung von Pauschaltarifen ("Flat-Rates") kann eine Speicherung zudem bisher gänzlich vermieden werden.

Der Arbeitskreis Vorratsdatenspeicherung ist ein bundesweiter Zusammenschluss von Bürgerrechtlern, Datenschützern und Internet-Nutzern, der die Arbeit gegen die geplante Vollprotokollierung der Telekommunikation koordiniert.

www.vorratsdatenspeicherung.de

Online-Flyer Nr. 72 vom 28.11.2006

<http://www.nrhz.de/flyer/beitrag.php?id=10361>

MAUS - 6.12.2006 um 15:40

LOL LOL LOL sorry, daß ich Euch schon wieder so nen endlangen Text vor die Füße knalle, aber der Bericht ist einfach zu geil (*g* ich liebe diese Zeitung), deshalb werde ich Passagen, die mir besonders gut gefallen auch mal farblich absetzen, vielleicht bekommt dann ja der ein oder andere doch Bock, sich alles durchzulesen...

[B]Verfassungsschützer demonstrieren gegen Umzug von Köln nach Berlin
Geheimdienstler als Rheinseparatisten
Von Hans-Detlev v. Kirchbach [/B]

"BFV bleibt in Köln und "Solidarität mit dem Verfassungsschutz". **Parolen** auf einer Demo und Kundgebung von - man mag's kaum glauben - VerfassungsschutzbeamtlInnen am 1. Dezember vor dem Kölner Rathaus, **die zeigen, daß die notorischen Ausspäher und professionellen Verdächtiger sozialer Protestbewegungen von ihrer "Klientel" gelernt haben** - zumindest von der Sprachform her.

"Der Kampf geht weiter!", rief denn auch der Kundgebungsleiter aus, ein Herr Jacobi, der als "Personalratsvorsitzender" im Bundesamt für Verfassungsschutz vorgestellt wurde. Da fehlt an sich nur noch die Straßenblockade oder die Besetzung der "Verfassungsschutz"-Zentrale durch die hauptamtlichen Inkriminatoren jeglicher unbotmäßiger Bürgeraktivität, deren Verdammung Umtriebe wie Sitzblockaden und Hausbesetzungen seit Jahrzehnten regelmäßig verfielen.

Was in der Weltsicht eines wackeren Verfassungsschützers eigentlich eine Störung der bestehenden Ordnung darstellt, die auf ewig registriert und nie verziehen, dem Normalverbraucher nach Jahrzehnten noch als „belastende Erkenntnis“ präsentiert wird, tun die beamteten Volksbeobachter nun selber: Sie gehen auf die Straße, sie demonstrieren, protestieren und pfeifen wütend, sobald der Name des Bundesinnenministers Schäuble oder seines Staatssekretärs, des Ex-BND-Präsidenten Hanning fällt. Einige von ihnen zeigten sich sogar nach Autonomienart verummmt, was bei anderen Demos sogleich die Polizei auf den Plan gerufen hätte, hier aber als natürliches Staatsschützer-Privileg durchging. Geraten die Stützpfiler der Inneren Sicherheit ins Wanken, von einer Seite her, die wir als vorverdächtige Normalbürger und gewöhnlicher Demonstrationspöbel nie für möglich gehalten hätten?

[B]Zwergenaufstand oder: Aufruhr der Staatsschützer[/B]

Vielleicht, denn es geht um das einzige Anliegen, für das ein ordentlicher deutscher Beamter überhaupt auf die Barrikaden gehen, womöglich sogar seinem Dienstherrn die Loyalität aufkündigen würde: die unanfechtbare Bequemlichkeit der eigenen Beamtenexistenz. Die aber sehen die Kölner Verfassungsschützer ausgerechnet durch Bundesinnenminister Schäuble in seiner abgehobenen Leichtfertigkeit und unter „Bruch ausdrücklicher Zusagen“ frevlerisch angegriffen. Ein Handschlag auf einem Viehmarkt sei mehr wert als ausdrückliche Zusagen des

Bundesinnenministern, zürnte Herr Jacobi unterm Jubel seiner KollegInnen. Die sind in der Tat stinksauer. Aus - in ihrer Sicht - gutem Grund: Beginnend mit ca. 250 "Experten" der "Abteilung VI", welche für den so genannten "Islamismus" zuständig ist, sollen in nächster Zeit die wohlbestallten Beamten des Inlandsgeheimdienstes ihr von uns allen nicht nur durch Dienstgehälter, sondern durch Dauerbespitzelung der Gesellschaft teuer bezahltes öffentliches Dienst-Sitzfleisch aus ihren komfortabel gepolsterten Chorweiler Amtsstubensesseln erheben. Denn im Sinne eines preußisch-autoritären, machtegeballten Zentralismus, wie ihn schon Schily geradezu fanatisch vertrat und Schäuble zu allem entschlossen nunmehr durchsetzt, sollen unsere Oberausspäher aus dem anheimelnden Karnevalsdorf am Rhein an die weit weniger idyllische Spree, in die eher unbehagliche Machtkapitale Berlin umziehen.

Dort will Schäuble mit langfristiger Konzentration und Vernetzung aller staatlicher Observations- und Repressionsmacht, insbesondere der Verschmelzung von Geheimdienst- und Polizeibehörden, das Projekt vollenden, von dem schon der ehemalige VS-Boß und Berliner CDU-Innensenator Ekkehart Werthebach tagträumte: das zentrale, keiner Machtbegrenzung mehr unterworfenen Bundessicherheitsamt. So jedenfalls benannte Werthebach sein ideelles Lieblingskind. Mag sein, daß Schäuble diesem Homunculus einer totalen Sicherheitsideologie vorerst noch einen leichter verdaulichen Tarnnamen geben wird, wie etwa "neue Sicherheitsarchitektur", "Synergienstruktur der Inneren Sicherheit" und ähnliche Ungetüme aus dem Politschwatzkasten. Mag auch sein, daß die Einzelbehörden als solche zunächst durchaus noch formal eigenständig bleiben, daß das Bundeskriminalamt also ebenso wie die 17 Bundes- und Landesämter für so genannten Verfassungsschutz ihre Namen ebenso behalten wie - besonders wichtig für mindestens 17 Spitzenbeamte - ihre "Präsidenten".

[B]Eigenheim-Mentalität wider Staatsarchitektur?[/B]

Doch in engster, von keinerlei Daten- und Persönlichkeitsschutz mehr ausgebreiteter, Verflechtung werden und sollen die expandierenden Agenturen der so genannten Inneren Sicherheit de facto einen einzigen funktionalen Organismus der Überwachung, Kontrolle, Verdächtigung der gesamten Bevölkerung bilden. Letztendliches Ziel ist, jede normwidrige Handlung, jede abweichende Strömung zu erkennen, zu benennen, zu beseitigen. Die so genannten Verfassungsschützer müssen also nach Berlin, auch in Zeiten virtueller Kommunikation, um diese "neue Sicherheitsarchitektur" auch topographisch und physisch zu repräsentieren.

Wie kleinformatig sind dagegen doch manche Argumente der protestierenden Verfassungsschützer, wie etwa: Man sei in Köln "heimisch" geworden, habe sich "Eigentum" und "Lebensmittelpunkte" aufgebaut. Mal abgesehen davon, daß die Verfassungsschützer auf die "Lebensplanungen" ihrer Observations- und Denunziationsopfer bislang auch noch nie Rücksicht genommen haben - Stichwort: Regelanfrage und Berufsverbote - verkennen solche kleinbürgerlichen Jammereien doch die Größe der historischen Aufgabe, die gerade Staatsschützern eigentlich einleuchten müßte.

Letztlich ist es nämlich ein fast religiöses Unterfangen, dem sich Schäuble, Schily vollendend, beherzt zuwendet: Der zentral grenzenlos ermächtigte totale Sicherheitsstaat. Der, selbst hinter einem Schleier der Geheimhaltung verborgen, alles sehen, alles hören, alles registrieren, alles im Zweifel sogleich sanktionieren soll, was der Plebs so tut und treibt. Insofern gehen die Warnungen vor einem „Zentralstaat“ auf der Kundgebung der rheinseparatistischen Verfassungsschützer genau in die richtige Richtung und trotzdem fehl. Denn die „neue“ Sicherheits- und Staatsarchitektur kann gar nicht anders als zentralistisch sein.

Da aber kann es einfach nicht hingehen, daß einzelne Mittel- und Oberbeamte einer ausschlaggebenden Überwachungsbehörde, die doch als einer der Stützpfeiler dieses gigantischen Sicherheitsgebäudes fungieren soll, aus privatistischer Kurzsichtigkeit und beamtentypischer Bequemlichkeit lieber in der Hauptstadt von Schunkeln und Frohsinn verbleiben wollen, statt wie ein Mann militärisch geordnet in die Metropole des neu aufgelegten deutschen Macht- und Ordnungsstaates abzumarschieren.

Im Zusammenhang mit der säkularen, ja transzendenten Bedeutung eben dieser gerade in Deutschland anscheinend unheilbar zeitlosen autoritären Staatsidee weisen solche Anwendungen von Familiensinn und Ortsverbundenheit, von Brauchtumsiebe, Bierseligkeit und FC-Fanatismus Züge einer nachgerade unverantwortlich menschlichen Normalität auf - und das ausgerechnet bei Geheimdienstlern. Vor dem Hintergrund des „höheren Auftrages“ schrumpfen freilich selbst die fest beamteten Führungsagenten jener geheimen Armee von inoffiziellen MitarbeiterInnen des Verfassungsschutzes, die uns auf Honorarbasis bis ins Privatleben hinein ausspähen, auf die Dimension kleiner Machtgehilfen. Die überschätzen vielleicht ihren Status, nur weil ihre Behörde aus eigener Machtvollkommenheit die politischen Aktivitäten der unverständigen Untertanen staatsverbindlich als verfassungsfeindlich abstempeln darf, wann immer das höhere Orts gewünscht wird. Oder weil Schäuble noch nach der Fußball-WM den Beitrag des Verfassungsschutzes zur Sicherheit dieses überwachungsstaatlichen Zentralevents geradezu hymnisch belobigte. Nun aber können die umzugsunwilligen VS-Bediensteten auf den Elitaristen Schäuble eigentlich nur als uneinsichtige Untergebene wirken, denen der Kopf zurechtgesetzt gehört.

Noch funktioniert der autoritäre Schily- und Schäuble-Staat allerdings nicht ganz so reibungslos, wie ihn sich seine Schöpfer wohl wünschen. Und so war eben eine der bizarrsten Demonstrationen der gesamten deutschen Demonstrationsgeschichte nicht vermeidbar: der öffentliche Auftritt einiger Hundertschaften von Verfassungs- "SchützerInnen" in der Rolle von Spontis, die dem Staat oder doch zumindest ihrem Minister den bösen Finger zeigten. Dabei wollen Vater Staats teure Kostgänger und treueste Wasserträger nur nicht aus ihrem Kölner Laufstall vertrieben werden, fort ins eisige, machtsstaatlich erwachsene Berlin.

[B]Volks(vertreter)bewegung für den Verfassungsschutz[/B]

Dafür können die verfassungsschützerischen Liebhaber der Rheinprovinz auf den Schutz rheinischer Provinzpolitiker rechnen, allen voran der Kölner OB Schramma und die örtliche SPD-Bundestagsabgeordnete Lale Akgün. OB Schramma weiß ja ohnehin, was angeblich alle Kölner wollen. Schon beim letztjährigen Rekrutengelöbnis unter dem Dom etwa hatte er, der Protestkulisse zum Trotz, alle Kölnerinnen und Kölner hochgerührt als LiebhaberInnen des Militärs ausgemacht.

Gleichermaßen begeistert sind die Kölner BürgerInnen vom Verfassungsschutz, das jedenfalls behauptete Schramma in seinem gut aufgelegten Büttensbeitrag vor den VerfassungsschützerInnen. „Wir alle vertrauen darauf, daß hier hervorragende Arbeit geleistet wird zum Schutz unserer Inneren Sicherheit“, verkündete er. „Hervorragende Arbeit“, wie sie das Bundesamt ja unter anderem mit dem NPD-V-Mann-Skandal „geleistet“ hat, aufgrund dessen das Bundesverfassungsgericht den NPD-Verbotsprozeß einstellen mußte. Derlei ficht den Obermeister aller Kölner Bürger allerdings nicht an. Ihm zufolge wünschen sich eine Million KölnerInnen nichts sehnlicher, als daß der Verfassungsschutz in Kölle bleibt. Denn, so der kölsche Volkstribun zum fast schon tränenfeuchten Abschluß seiner Rede: „Mer all sinn Kölle.“ Begeisterter Applaus der VerfassungsschützerInnen, die allerdings im wesentlichen unter sich blieben; die in Anspruch genommenen Kölner BürgerInnen verirrt sich nicht auf diese Kundgebung.

Freilich ließ sich die SPD-Volksvertreterin Lale Akgün in ihrer Zuneigung für die Volksüberwachungsbehörde von der Begeisterung des CDU-OB Schramma für das Bürgeraushorchart nicht übertreffen. Als "Islam-Beauftragte" der SPD-Bundestagsfraktion machte sie den Hauptfeind im "Islamismus" aus - das "Operationsgebiet" für diese Feindlage aber sei eben nicht im Osten und Berlin, sondern hier im Westen. Hier konzentrierten sich für die "hervorragenden Experten" des VS die "Beobachtungsobjekte". Mit welchem Unwort aus der Schreckenskammer von Polit- und Bürokratensprache natürlich Menschen gemeint sind, nämlich solche, die von rasterfahndendem staatsschützerischem Vorverdacht mit dem Etikett potentieller Terrorismusneigung behaftet werden. Wofür genügt, daß sie aus suspekten orientalischen Weltgegenden stammen und daher ihren „Gott“ mutmaßlich anders buchstabieren als Joachim Kardinal Meisner oder Bundesfamilienministerin Ursula von der Leyen. Wie etwa jener harmlose Ingenieursstudent aus einem verdächtigen Herkunftsland, der kürzlich die nachträgliche Mitteilung erhielt, er sei, weil erstens Afghane und zweitens Student, in die Rasterfahndung nach islamistischen „Schläfern“ einbezogen worden.

Das ist ja das Schöne an den Doktrinen zur Bekämpfung des Bösen, wie sie gerade in der Abteilung sechs des Bundesamtes für Verfassungsschutz mit entwickelt worden sind: Verdächtig sind gerade die Unauffälligen, die immer so harmlos tun. Die nicht einmal demonstrieren und den Bundesinnenminister abwatschen wie die aufgebrachten VerfassungsschützerInnen vor dem Kölner Rathaus. Ob es über diese DemonstrantInnen inzwischen auch schon eine Akte beim Verfassungsschutz gibt? -

[B]Sag zum Abschied leise Servus[/B]

Noch wichtiger aber scheint die Frage: Was aber sollen wir Kölner BürgerInnen dazu meinen, wenn wir uns von unserem OB nicht einfach widerspruchslos in den Fanclub des Verfassungsschutzes eingemeinden lassen wollen? Zum einen möchte man den Protest der Verfassungsschützer gerne unterstützen, nicht, weil sie peinlich sentimental ihre Liebe zu Karneval und FC in einem via Internet verbreiteten Video bekunden - von dem sich aber Herr Jacobi distanzierte, da er "uns nicht von interessierter Seite als Karnevalsveranstaltung lächerlich gemacht" sehen wollte. Einerseits die vollmundigen Bekenntnisse zu Köln („Das Bundesamt gehört zu Köln wie der Dom“, so Jacobi), andererseits aber die plötzliche Distanzierung vom Karneval - das geht irgendwie nicht zusammen.

Allerdings geht die ganze Heimattümelei aber auch zumindest dem Kommentator als prinzipiell heimatlosem Kölner Zweck-Immi völlig dort vorbei, worauf die besoldeten Damen und Herren in ihrer Chorweiler Behörde ansonsten sitzen. Sympathisch könnte der Protest der kölnanhänglichen Verfassungsschützer jenseits jeglichen Lokalpatriotismus vielmehr aus einem ganz anderen Grund erscheinen: weil sie, ausgerechnet sie, mit ihrer fast kindlichen Trotzhaltung zumindest ein kleines Sandkorn in Schäubles autoritär-staatliches Getriebe werfen.

Andererseits könnte man auch eine gewisse Erleichterung darüber empfinden, daß Köln demnächst eine Zentralinstitution des totalen Überwachungsstaates und etwa 1.000 Schnüffel- und Spitzelprofis weniger beheimaten

wird. Und das mag sogar die 100 Millionen Euro wert sein, die nach Meinung der protestierenden VS-Beamten ein Umzug ihrer Behörde nach Berlin kosten würde.

Online-Flyer Nr. 73 vom 05.12.2006

<http://www.nrhz.de/flyer/beitrag.php?id=10379>

MAUS - 11.12.2006 um 14:06

11.12.2006 10:34

[B]Webdemo zum "Trauertag um das Fernmeldegeheimnis" [/B]

Der Arbeitskreis Vorratsdatenspeicherung hat wegen des Jahrestags des Beschlusses zur Einführung der "Totalprotokollierung" der elektronischen Nutzerspuren zur Verhüllung von Webseiten am 14. Dezember aufgerufen. 2005 segnete die "große Koalition" aus Konservativen und Sozialdemokraten im EU-Parlament nach einem kurzfristig von den Fraktionsspitzen verabredeten Kompromiss die heftig umstrittene Richtlinie zur verdachtsunabhängigen Vorratsspeicherung von Telefon- und Internetdaten ab. Gleichzeitig haben die Abgeordneten nach Ansicht der Bürgerrechtsorganisation die Maxime im Grundgesetz "Das Fernmeldegeheimnis ist unverletzlich" zu Grabe getragen. Am Donnerstag sollen daher Betreiber von Webseiten unter dem Motto "Stoppt die Vorratsdatenspeicherung! Gläsernes Telefon, Handy, E-Mail und Internet" darauf aufmerksam machen, dass künftig aber die Aufzeichnung "sämtlicher Kommunikationsvorgänge zum Normalfall werden soll".

Ein nachdrücklicher Appell des Arbeitskreises geht zudem an "die Medien", die Menschen über die Einführung der Verpflichtung von Telcos zur anderthalb bis zweijährigen Vorhaltung von Verbindungs- und Standortdaten zu informieren und die Bürger besser über die Folgen der tief in die Grundrechte einschneidenden Maßnahme zu unterrichten. "Obwohl dieses Vorhaben die Grundlagen unserer freien Gesellschaft in Frage stellt, fallen die Massenmedien als Informationsmittel der Bürger bisher weitgehend aus", beklagt der Jurist Patrick Breyer von der zivilgesellschaftlichen Vereinigung. Er fürchtet ein gesellschaftliches Klima der Überwachung und Störungen der Kommunikation in sensiblen Angelegenheiten. Die meisten Leute wissen ihm zufolge aber noch nicht, dass ein Großteil ihres Privatlebens ab Herbst 2007 nachvollziehbar werden soll. Der Arbeitskreis ruft daher auch Bürger, die bereits im Bilde über die Vorratsdatenspeicherung und darüber besorgt sind, auf, von ihrer Zeitung, Lieblingszeitschrift oder -fernsehsendung eine Berichterstattung über den "1. Todestag des Telekommunikationsgeheimnisses" einzufordern. Einen Musterbrief zum Versand an die Medien sowie auch einen Code für die Webdemo stellt die Organisation auf ihrer Internetseite bereit.

Bundesjustizministerin Brigitte Zypries (SPD) hat vor kurzem einen Gesetzentwurf zur Einführung der Vorratsdatenspeicherung in Deutschland vorgelegt, die nach Ansicht von Datenschützern einen "Paradigmenwechsel" mit sich bringen und die Unschuldvermutung ad absurdum führen würde. Der Arbeitskreis hält die Pläne für verfassungswidrig und fordert ihre Aufgabe, zumal der Europäische Gerichtshof (EuGH) nächstes Jahr über eine von Irland eingereichte Nichtigkeitsklage gegen die Richtlinie zur Vorratsdatenspeicherung entscheiden werde. Für den Fall, dass die große Koalition von ihren Plänen keinen Abstand nimmt, organisiert der Arbeitskreis Vorratsdatenspeicherung eine "Sammel-Verfassungsbeschwerde". Bereits 7000 Bürger wollen sich daran beteiligen, unter anderem auch die stellvertretende Vorsitzende der Fraktion der Linkspartei, Petra Pau. Mit der pauschalen Überwachungsmaßnahme können ihrer Ansicht nach "Kontakte verfolgt und Profile erstellt werden. Betroffen sind der Datenschutz, die Pressefreiheit sowie weitere Grundrechte." Pau betont daher im Einklang mit den Bürgerrechtlern: "Ich halte das Vorhaben schlicht für grundgesetzwidrig."

<http://www.heise.de/newsticker/meldung/82322>

MAUS - 11.12.2006 um 14:16

[B]Chaos Computer Polizei

KOMMENTAR VON Christian Rath[/B]

Die Methoden der Polizei werden immer verwegener. Inzwischen versuchen die Ermittler sogar mit Hilfe von Hacker-Software auf private PCs Zugriff zu nehmen. Die Festplatten werden durchsucht, ohne dass der Benutzer davon etwas merkt. Dem hat der Bundesgerichtshof (BGH) jetzt vorläufig einen Riegel vorgeschoben: Die Online-Durchsuchungen sind illegal, weil es keine gesetzliche Grundlage gibt. Das ist eine erfreuliche und überfällige Entscheidung - denn bisher drückte der BGH mehr als ein Auge zu.

Unangenehm ist die Entscheidung für Innenminister Schäuble. Ein wichtiger Punkt in seinem Programm zur Stärkung der inneren Sicherheit war, die Polizei mit besserer Hacker-Software auszustatten. Das Programm wurde ziemlich

kurzfristig in den letzten Bundeshaushalt aufgenommen und den Innenpolitikern nur ganz kurzfristig vorgestellt. Besorgten Abgeordneten beschied die große Koalition, dass das PC-Screening rechtlich völlig unproblematisch sei. Von wegen. Zwei Tage nach der fraglichen Bundestagsdebatte kam die Ohrfeige vom Bundesgerichtshof aus Karlsruhe.

Wenn der BGH nicht noch einknickt, wird Schäuble sicher versuchen, sich vom Bundestag eine gesetzliche Grundlage zu besorgen. Die wird er, wie man die große Koalition kennt, wohl auch bekommen. Aber ist damit alles in Ordnung? Dass die Polizei hier etwas tut, was Privaten verboten ist, spricht nicht gegen ein derartiges Gesetz. Das gilt schließlich für fast alle Polizeimaßnahmen, von der Verhaftung bis zum Abhören von Telefonen. Wichtig ist aber, dass die Maßnahme nur bei schwerster Kriminalität und bei dringendem Tatverdacht zugelassen wird. Der Kernbereich der privaten Lebensführung muss gewahrt bleiben. Schließlich ist der private PC für viele Menschen auch eine Art Tagebuch.

Ist es nicht möglich, solche Bereiche bei einer heimlichen Ausforschung zu schützen, dann muss Schäuble auf diese Maßnahme verzichten und wie bisher offen die Wohnung durchsuchen. Der Betroffene kann dann vor Ort mit der Polizei verhandeln, welche Teile ihrer Festplatte für sie tabu bleiben sollen. So viel Takt muss sein - auch bei der Verfolgung von Terroristen.

der tag SEITE 2

taz vom 11.12.2006, S. 1, 62 Z. (Kommentar), Christian Rath

<http://www.taz.de/pt/2006/12/11/a0053.1/text>

[B]Computer-Screening vorerst gestoppt [/B]

Berlin (NRhZ/DL, 11.12.) Der Bundesgerichtshof hat die polizeiliche Praxis der Online-Durchsuchungen für illegal erklärt. Dazu erklärt Petra Pau, stellvertretende Vorsitzende der Fraktion DIE LINKE. und Mitglied im Innenausschuss: „Ich begrüße das Urteil, denn die heimliche Online-Durchsuchung von Home-Computern (Computer-Screening) greift tiefer in die Privat-Sphäre ein, als eine genehmigte Hausdurchsuchung. Durch Online-Untersuchungen wird das Grundrecht auf informationelle Selbstbestimmung hinterrücks und klammheimlich gebrochen.“ - Bei Online-Untersuchungen hackt sich die Ermittlungsbehörde in den Computer der betroffenen Person ein und kann so prüfen, welche Texte, Bilder, e-mails usw. auf ihm gespeichert sind. Das geschieht mittels "Trojanern" oder unter Ausnutzung von Sicherheitslücken in installierten Programmen.

http://www.nrhz.de/flyer/suche.php?ressort_id_menu=-1&ressort_menu=News

MAUS - 16.12.2006 um 03:04

15.12.2006 12:28

[B]

Brandenburg erhält deutlich verschärftes Polizeigesetz [/B]

Der Brandenburger Landtag hat mit den Stimmen der schwarz-roten Regierungskoalition am gestrigen Donnerstag eine heftig umstrittene Novelle des Polizeigesetzes verabschiedet. Sie gibt Ermittlern zahlreiche neue Befugnisse in die Hand. So dürfen die Gesetzeshüter in der Mark künftig den großen Lauschangriff in Form der akustischen Wohnraumüberwachung präventiv und bei "Gefahr im Verzug" ohne richterliche Genehmigung durchführen. Auch sonst genügt hier der Segen eines einzigen Amtsrichters, während bislang die Erlaubnis von mehreren Landesrichtern erforderlich war. Ohne richterliche Genehmigung darf die Polizei ferner künftig Handys zur "Gefahrenabwehr" mit dem IMSI-Catcher orten. Generell darf sie ohne Anfangsverdacht auch Telekommunikationsvorgänge verhindern oder unterbrechen, was frühzeitig den Branchenverband Bitkom auf den Plan gebracht hatte.

Weiter wird die an vier Jahren über fünf Jahre hinweg erprobte Videoüberwachung umfassend gesetzlich festgeschrieben und ausgeweitet. Sie wird an allen öffentlich zugänglichen, besonders gefährdeten Orten zulässig. Die Aufzeichnungen dürfen bis zu 48 Stunden gespeichert werden. Dazu kommt eine "anlassbezogene Kennzeichenfahndung". Sie soll es in einer akuten Bedrohungslage ermöglichen, den Durchgangsverkehr schnell und automatisch auf gesuchte Kfz-Nummernschilder hin zu kontrollieren. Konkret sollen nach Informationen der Welt an Brandenburgs Autobahnbrücken Spezialkameras angebracht werden, welche die Kennzeichen aller vorbeifahrenden Autos erfassen. Die Daten sollen dann sofort mit denen gesuchter Fahrzeuge abgeglichen werden.

Die geplante Ausweitung der polizeilichen Überwachungsmöglichkeiten war im Vorfeld auf große Proteste gestoßen. Der

Anwaltsverein hatte bei einer Anhörung im November gewarnt, die geplanten Regelungen zum Lauschangriff und zur "vorbeugenden Telefonüberwachung" seien "schlicht verfassungswidrig". Brandenburg übernehme eine Regelung aus Niedersachsen, die das Bundesverfassungsgericht bereits 2005 kassiert habe. Der Innenexperte der Fraktion der Linken im Landtag, Hans-Jürgen Scharfenberg, gab vergangene Woche zu bedenken, dass Menschen bei der Verabschiedung des Gesetzes künftig Beobachtung und Abhörmaßnahmen ausgesetzt seien, "egal, ob sie durch ihr Handeln dazu irgendeinen Anlass gegeben haben oder nicht." Auch die brandenburgische Datenschutzbeauftragte Dagmar Hartge hatte das Vorhaben im Lauf der Woche noch einmal scharf kritisiert.

Schon der Kabinettsbeschluss im Sommer war verzögert worden, da Finanzminister Rainer Speer (SPD) zunächst seine "liberalen Grundsätze" im Änderungsentwurf nicht mehr gewahrt sah. Die Mehrheit in der SPD gab sich später aber damit zufrieden, dass zwei Regelungen auf Probe erfolgen. So sind die Handy-Ortung sowie die Kennzeichenüberwachung zunächst auf zwei Jahre befristet. Nichtsdestoweniger lehnten bei der gestrigen Schlussabstimmung die SPD-Abgeordneten Tina Fischer, Jens Klocksinn und Andreas Kuhnert die Reformvorlage als unangemessen ab. Ihre Parteikollegen Martina Münch und Esther Schröder enthielten sich.

Die Linken und die rechtsextreme DVU stimmten gegen die Gesetzesänderung. Scharfenberg warf der Regierung Populismus vor, das sie mit der "subjektiven Kriminalitätsfurcht" der Bürger Politik mache. Der Preis sei eine "kaum umzukehrende Aushöhlung der Grundrechte". Die rot-schwarze Koalition dehne ohne Not die Überwachungsmöglichkeiten aus, denn die Kriminalität habe in Brandenburg während der vergangenen zehn Jahre um etwa 30 Prozent abgenommen. Eine Auswertung des Videoüberwachungsprojekts habe jedoch ergeben, dass die Kriminalität in angrenzenden Bereichen gestiegen sei. Innenminister Jörg Schönbohm (CDU) betonte dagegen, die Sicherheit der Bürger müsse gewährleistet werden. Das Gesetz sei rechtsstaatlich einwandfrei und vor allen Maßnahmen gebe es hohe juristische Hürden. (Stefan Krempel) / (jk/c't)

<http://www.heise.de/newsticker/meldung/82598>

:60:

MAUS - 16.12.2006 um 03:10

15.12.2006 12:05

[B]Bundesrat winkt Telekommunikationsgesetz und Anti-Terrorgesetze durch [/B]

Die Länderchefs hatten es am heutigen Freitag eilig, die umstrittene Änderung des Telekommunikationsgesetzes (TKG) im Bundesrat passieren zu lassen. Nachdem der nordrhein-westfälische Minister für Bundes- und Europa-Angelegenheiten Michael Breuer sowie der parlamentarische Staatssekretär im Bundeswirtschaftsministerium Hartmut Schauerte noch einmal für die ausgeglichenen Regelungen geworben hatten, stimmte der Bundesrat für die Novelle. Ein Antrag des federführenden Wirtschaftsausschusses, mit dem das Gesetz als "nicht EU-rechtskonform" kritisiert werden sollte, fand keine Mehrheit. Um das Inkrafttreten der TKG-Reform nicht zu verzögern, widersetzten sich die Landesfürsten auch dem Begehrt des Rechtsausschusses, wegen der 2003 ins TKG aufgenommenen Klausel zur Entschädigung von Telcos und Providern für ihre Hilfsleistungen bei staatlichen Überwachungsmaßnahmen den Vermittlungsausschuss anzurufen.

Besonders umkämpft ist die Gesetzesänderung, weil sie "neue Märkte" für unbestimmte Zeit von der Regulierung freistellen will. Die damit einhergehenden Regulierungsferien für das VDSL-Netz der Deutschen Telekom werden von Wettbewerbern und Oppositionspolitikern als Signal zur erneuten Monopolisierung des Telekommunikationssektors scharf kritisiert. Auch die EU-Kommission hat wiederholt angekündigt, bei Inkrafttreten des Gesetzes ein Vertragsverletzungsverfahren gegen die Bundesregierung anzustrengen. Der Ende vergangene Woche aufgeloderte Widerstand von Ländern wie Hamburg oder Niedersachsen gegen die Bestimmung erlosch im Vorfeld der Abstimmung wieder. Auch die Bedenken der Wirtschaftspolitiker, die zumindest in einem Zusatzprotokoll dokumentiert werden sollten, bügeln die Länderchefs weg.

Der Wirtschaftsausschuss hatte moniert, dass die gesetzlichen Vorgaben einzelne Regulierungsziele vorzögen und der Kriterienkatalog zur Definition neuer Märkte zu schwammig sei. Er beklagte ferner, dass es Eingriffsmöglichkeiten für den Regulierer erst bei langfristigerer Wettbewerbsbehinderungen geben soll. Damit würde die angestrebte Klausel die "ordnungspolitische Zweckbestimmung des EU-Rechtsrahmens" und die darin getroffenen Befugnisse der Bundesnetzagentur zur Marktanalyse konterkarieren. Darüber hielten die Wirtschaftspolitiker auch eine "effiziente Ausgestaltung der nachträglichen Entgeltregulierung und der besonderen Missbrauchsaufsicht" für "dringend

notwendig".

Ohne jegliche Einwände hat der Bundesrat zudem die neuen, vom Bundestag mit schwarz-roter Mehrheit Anfang Dezember beschlossenen Anti-Terrorgesetze abgenickt. Es geht dabei zum einen um die Befugnis für das Bundeskriminalamt, von Januar an eine zentrale Anti-Terrordatei einzurichten und dabei vorhandene Datenbestände von Polizeien und Geheimdiensten zusammenzuführen. In Kraft treten kann zudem das volksnah betitelte Terrorismusbekämpfungsergänzungsgesetz (TBEG), das die den Geheimdiensten nach dem 11. September gegebenen erweiterten Befugnisse verlängert und erneut ausdehnt.

Neben dem Verfassungsschutz können so künftig auch Bundesnachrichtendienst (BND) und Militärischer Abschirmdienst (MAD) Auskünfte bei Luftfahrtunternehmen, Banken, Post-, Telekommunikations- und Telediensteunternehmen einholen. Dies gilt nicht mehr nur bei Terrorverdacht, sondern auch im Rahmen der Aufklärung "verfassungsfeindlicher Bestrebungen" im Inland. Entsprechend ausgedehnt wird die Ermächtigung zum Einsatz des IMSI-Catchers für die Mobilfunküberwachung. Verdeckt fahnden dürfen Sicherheitsbehörden ferner im Schengener Informationssystem. (Stefan Krempl) / (jk/c't)

<http://www.heise.de/newsticker/meldung/82597>

MAUS - 29.12.2006 um 13:32

[B]Hacker im Staatsauftrag [/B]

Berlin (NRhZ/DL, 20.12.) Der nordrhein-westfälische Verfassungsschutz darf in Zukunft private Computer heimlich online durchsuchen. Damit erlaubt die Landesregierung dem Geheimdienst, seine Angriffe auf demokratische Grundrechte zu verstärken. Zu dem heute vom Landtag beschlossenen neuen Verfassungsschutzgesetz erklärt Ulla Jelpke, innenpolitische Sprecherin der Fraktion DIE LINKE. und Mitglied der Landesgruppe NRW: "Online-Schnüffeleien gehören zum perfidesten Repertoire von Geheimdienstlern, weil sie am helllichten Tag geschehen und doch unsichtbar sind. Den Bürgerinnen und Bürgern werden gleich mehrere Grundrechte vorenthalten." Verantwortlich für das Gesetz ist FDP-Innenminister Ingo Wolf.

http://www.nrhz.de/flyer/suche.php?ressort_id_menu=-1&ressort_menu=News

[B]Verfassungsschutz überwacht komplette Linksfraktion [/B]

Berlin (NRhZ/DL, 22.12.) Der Verfassungsschutz bespitzelt offensichtlich die komplette Linksfraktion. Das gehe aus der Antwort auf eine Kleine Anfrage der Fraktion hervor, wie deren innenpolitische Sprecherin Ulla Jelpke heute mitteilte. Laut Ulla Jelpke bestätigt die Bundesregierung darin, dass Informationen über die parlamentarische Tätigkeit der Abgeordneten "sach- und personenbezogen in einer diesbezüglichen Sachakte festgehalten" werden. Als Zweck der Bespitzelung werde genannt, "Bestrebungen gegen die freiheitliche demokratische Grundordnung" entgegenzutreten. Dabei werde den Abgeordneten der Linksfraktion unterstellt, es gebe "tatsächliche Anhaltspunkte für linksextremistische Bestrebungen". Jelpke nennt die Überwachung einen Skandal. Damit würden „über vier Millionen Wählerinnen und Wähler in die extremistische Ecke gestellt, ohne auch nur einen Anhaltspunkt für irgendwelche extremistischen Bestrebungen der Linken nachweisen zu können.

http://www.nrhz.de/flyer/suche.php?ressort_id_menu=-1&ressort_menu=News

[B]28.12.2006 11:18

23C3: "Sind wir paranoid genug?" [/B]

Experten haben auf dem 23. Chaos Communication Congress in Berlin am Mittwoch ein detailreiches Bild über den Stand staatlicher und privater Überwachung gemalt, die auch vor Hotelräumen, dem Internet und privaten PCs nicht haltmacht. "Die Frage muss lauten: Sind wir paranoid genug?", sagte der Coburger Sicherheitsberater Manfred Fink.

Fink empfahl allen, die in Hotelzimmern Wert auf Privatsphäre legten, "kritische Geräte" wie Telefone, Fernsehgeräte oder Radiowecker zu entfernen. Ein Auge sollte man auch auf die Schächte für die Klimaanlage haben, da dahinter Kameras versteckt sein könnten. Es gebe gerade in Luxusherbergen zahlreiche "verborgene Infrastrukturen", warnte

Fink. Er empfahl, "einfach mal gegen die Decke zu drücken". Mitgebracht hatte der Wanzenjäger unter anderem eine Kachel mit dahinter installiertem Mini-Elektroauge.

Hotelzimmer gehören laut Fink "zu den unsichersten Orten überhaupt", was die Vertraulichkeit von Kommunikation anbelangt. Sie böten Informationsbeschaffern ein leichtes Spiel. In einer fremden Umgebung sei der Aufwand groß, Abhörsicherheit herzustellen. Er riet davon ab, in Hotels Telekommunikationsanlagen ohne vertrauenswürdige Verschlüsselungstechniken zu benutzen und öffentliche WLAN-Netze in Anspruch zu nehmen. Generell sei es hilfreich, nicht alle Dinge bei einem Telefonat im Klartext zu benennen. Bei E-Mails sollten vertrauliche Informationen mit Hilfe der Steganographie im Datenwust etwa eines Bildanhangs versteckt werden. Dies habe zugleich den Vorteil, dass damit eventuell bestehende Kryptographieverbote umgangen werden könnten. Faxe sollten handschriftlich diagonal beschrieben werden, um die OCR-Scansoftware der Lauscher auszutricksen.

Dass der Aufwand bei Bedarf angemessen sei, illustrierte Fink anhand von Medienberichten etwa über die audiovisuelle Überwachung im Hotel "Neptun" in Warnemünde und anderen von der Stasi unterwanderten Absteigen im ehemaligen Osten. 1997 sei aber auch aufgefliegen, dass im Marriott-Hotel in Wien in der Nähe des OPEC-Gebäudes drei Luxussuiten mit professionell ferngesteuerten Raumwanzen für Langwellenfunk ausgerüstet waren. In Verdacht, die Mikros installiert zu haben, geriet damals die National Security Agency (NSA), der technische Geheimdienst der USA.

Als Überwachungstrend machte Fink das Einschleusen präparierter Akkus in Mobiltelefone aus. Dazu reiche es aus, das Handy kurzzeitig unbeaufsichtigt zu lassen. In seiner Firma seien beim Röntgen mit hochauflösenden Digitalsystemen mehrere hundert Geräte mit Wanzen-Akkus entdeckt worden. "Machen Sie Kerben oder Kratzer rein", empfahl der Sicherheitsberater. Er schätzte die Anzahl der Geheimdienstler und Strafverfolger, die sich auf derlei Abhöraktionen spezialisiert hätten, auf "hoch dreistellig".

Der Kölner Strafrechtler Marco Gercke warnte davor, Regierungen als Sicherheitsgaranten in einer Welt ständig heraufbeschworener terroristischer Akte zu sehen. "Wir können Regierungen nicht trauen, wir müssen sie kontrollieren", betonte Gercke unter dem Beifall der Hackergemeinde. Dies sei heutzutage umso nötiger, als die Gesetzgeber nicht mehr auf Experten hörten. Vielmehr würden sie ihre Entwürfe von Konzernen schreiben lassen, wie etwa die Urheberrechtsreform zeige. "Know your Citizens", beschrieb der Wissenschaftler das Motto von Regierungen im digitalen Zeitalter. Das Spektrum gehe von der verdachtsunabhängigen Vorratsdatenspeicherung über Volkszählungen, die Erfassung von Kfz-Kennzeichen, Videoüberwachung, Mautsysteme bis hin zu Ausweisdokumenten, die nun mit der Funktechnik RFID und Fingerabdrücken aufgerüstet würden.

Im vergangenen Jahr hatte Gercke auf dem Hackerkongress prophezeit, dass die Sicherheitsbehörden auf Befugnisse zum Eindringen in private Rechner mit Hilfe von Trojanern drängen und per Keylogger sämtliche Tastatureingaben der PC-Nutzer mitschneiden wollten. Inzwischen hat Nordrhein-Westfalen ein entsprechendes Gesetz für solche "Online-Durchsuchungen" verabschiedet, während Bundesinnenminister Wolfgang Schäuble auf eine bundesweite Regelung pocht. Die Prinzipien der Hausdurchsuchung seien aber nicht aufs Internet übertragbar, warnte Gercke. Insgesamt bezeichnete er Versuche zur vorsorglichen Straftatenabwehr als "Nonsens". (Stefan Krempf) / (cp/c't)

<http://www.heise.de/newsticker/meldung/83002>

MAUS - 3.1.2007 um 12:26

02.01.2007 08:27

[B]Bundesdatenschützer fordert Nachbesserungen zu Telefonüberwachung [/B]

Der Bundesdatenschutzbeauftragte Peter Schaar hat Nachbesserungen bei der geplanten Neuregelung der Telefonüberwachung gefordert. "Die Abgrenzungen zwischen dem Erhebungs- und Verwertungsverbot von Aufzeichnungen müssen deutlicher getroffen werden", sagte Schaar der Berliner Zeitung. "Das Gesetz sollte festlegen, wann die Polizei das Abhören abbrechen muss, und in welchen Fällen Informationen zwar gewonnen, aber nicht für die Ermittlungen verwertet werden dürfen."

Schaar monierte, dass das geplante Gesetz ein Erhebungsverbot nur dann vorsehe, wenn das Gespräch ausschließlich den Kernbereich der Privatsphäre betrifft. "Praktisch bedeutet dies, dass in keinem Fall auf das Abhören verzichtet wird", sagte er. "Das geht zu weit. Ich halte diese Regelung für unvereinbar mit den Vorgaben des Verfassungsgerichts."

Schaar warnte zudem davor, dass Privatfirmen Zugang zu der geplanten Speicherung von Telefon-, Handy- und Internetdaten erhalten. "Es geht bei der Vorratsdatenspeicherung längst nicht mehr nur um die Terrorismusbekämpfung, sondern auch um Wirtschaftsinteressen." Als Beispiel nannte Schaar die Musik- und die Filmindustrie. Diese wolle Zugriff

auf diese Daten, um so an die Personen zu kommen, die etwa über Internet-Tauschbörsen urheberrechtlich geschützte Werke weiter geben. Schaar bekräftigte seine grundsätzliche Kritik an dem geplanten Vorhaben des Bundesjustizministeriums.

Der Bundesdatenschutzbeauftragte warnte auch vor einer generellen Internet-Überwachung durch die Polizei. "Eine generelle Internet-Überwachung darf es nicht geben." Nur wenn es konkrete Anhaltspunkte auf Straftaten oder Gefährdungen gebe, dürfe die Polizei im Internet fahnden. "Aber ein generelles Einloggen in Chats ohne Hinweis auf eine Straftat halte ich für problematisch." (dpa) / (jk/c't)

<http://www.heise.de/newsticker/meldung/83079>

MAUS - 6.1.2007 um 13:52

05.01.2007 16:27

[B]Linkspartei sieht "Terrorismusbekämpfung" als Hebel für Telefonüberwachung [/B]

Im Jahr 2005 wurden in Deutschland gegen 50 Beschuldigte Ermittlungsverfahren wegen Verdachts auf terroristische Aktivitäten eröffnet. Zugleich hat es fünf Verurteilungen wegen Verstoßes gegen die Bestimmungen des Paragraphen 129 StGB gegeben. Neu hinzu kamen sieben Anklageerhebungen. Das geht laut Mitteilung von Ulla Jelpke, innenpolitische Sprecherin der Bundestagsfraktion Die Linke, aus der Antwort der Bundesregierung auf eine Kleine Anfrage zur Anwendung der Paragraphen 129, 129a und 129b hervor. Im Kontrast zur Zahl der Verurteilungen stehe die Zahl von 33 Telekommunikationsüberwachungen, von denen 148 Personen betroffen waren.

"Man muss davon ausgehen, dass solche Verfahren häufig nur deswegen angestrengt werden, um das Umfeld bestimmter Personen ausleuchten zu können, ohne dass es konkrete Hinweise auf Straftaten gibt", meint Jelpke. Die Terrorismusbekämpfung sei für Bundeskriminalamt und Bundesanwaltschaft in erster Linie ein Hebel zur Telefonüberwachung. Zudem blieben Neonazis von diesen Verfahren praktisch verschont. "Das Bundesamt für Verfassungsschutz hat 2005 von verschiedenen Waffenfunden und Wehrsportgruppen berichtet. Dem steht ein einziges Ermittlungsverfahren gegen unbekannte rechtsterroristische Täter gegenüber", erläutert Jelpke. (anw/c't)

<http://www.heise.de/newsticker/meldung/83259>

MAUS - 21.1.2007 um 16:12

18.01.2007 17:11

[B]Verfassungsbeschwerde gegen neues Telemediengesetz angekündigt [/B]

Die Mülheimer Journalistin und Autorin Bettina Winsemann alias Twister will wegen der Überwachungsklauseln im gerade vom Bundestag verabschiedeten Gesetz zur Neuordnung des Medienrechts nach Karlsruhe ziehen. Die Bürgerrechtlerin sieht im neuen Telemediengesetz (TMG), das den Kern des Elektronischen Geschäftsverkehr-Vereinheitlichungsgesetzes (EIGVG) ausmacht, einen weiteren Stein in einer Mauer von Bespitzelungsvorhaben der großen Koalition, welche "die Privatsphäre und den Datenschutz abblocken". Die Freiberuflerin hat erst vor kurzem eine Verfassungsbeschwerde auch gegen das neue Verfassungsschutzgesetz in Nordrhein-Westfalen initiiert, das eine Rechtsgrundlage für verdeckte "Online-Durchsuchungen" privater Internet-PCs durch Geheimdienste schafft.

Vorgehen will Twister mit der weiteren angekündigten Verfassungsbeschwerde vor allem gegen Paragraph 14 TMG, der ihrer Ansicht nach Privaten einen direkten Auskunftsanspruch über Nutzerdaten gegenüber den Anbietern von Telemediendienste einräumt und damit den Schutz der Privatsphäre aushöhlt. "Dass Lobbyisten die Verfolgung von Urheberrechtsverletzungen in einem Atemzug mit den Aufgaben der Geheimdienste nennen, ist ein Skandal", empört sich die Bürgerrechtlerin. "Dass diese Formulierung nun aber Eingang in ein Gesetz findet, ist weitaus skandalöser." Damit würden sich Regierung und Parlament zum Handlanger für private Interessensvereinigungen machen.

Werner Hülsmann, Vorstand der Deutschen Vereinigung für Datenschutz (DVD), will die Beschwerde gemeinsam mit Twister führen: "Mit der beschlossenen Verwendung der Internetnutzungsdaten zur 'polizeilichen Gefahrenabwehr' und bei privatrechtlichen Auskunftsansprüchen im Urheberrechtsbereich werden Scheunentore geöffnet, ohne dass Verfahrensregelungen aufgestellt würden, die datenschutzrechtlichen Mindeststandards genügen würden", erläutert er seine Beweggründe zur Unterstützung der Klage. "Dieses Vorgehen ist verfassungsrechtlich nicht haltbar und stellt einen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung der Internetnutzer dar."

Die beiden Aktivisten engagieren sich auch im Arbeitskreis Vorratsdatenspeicherung und sehen durch Gesetze dieser

Art die Privatsphäre und die demokratischen Beteiligungsmöglichkeiten aller Bürger in hohem Maße gefährdet. "Die gesamte Diskussions- und Informationskultur wird leiden, wenn eine unüberwachte Kommunikation kaum mehr möglich ist", gibt Twister zu bedenken. Die Bürgerrechtlerin reibt sich vor allem auch daran, dass nunmehr schon "das Herunterladen von bestimmten Informationen quasi einen Anfangsverdacht darstellen soll". Ähnliche Sorgen hatten Datenschützer bereits bei einer Anhörung zum TMG im Bundestag Mitte Dezember geäußert.

Der besonders umstrittene Absatz im Telemediengesetz sieht vor, dass die erfassten Anbieter künftig Informationen wie Name, Anschrift oder persönliche Nutzerkennungen auch für Präventionszwecke herausrücken müssen. Die Provider werden verpflichtet, "für Zwecke der Strafverfolgung, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder zur Durchsetzung der Rechte am geistigen Eigentum und zur Gefahrenabwehr durch die Polizeibehörden der Länder" die entsprechenden Daten weiterzugeben. (Stefan Krempf) / (pmz/c't)

<http://www.heise.de/newsticker/meldung/83920>

MAUS - 24.1.2007 um 13:13

[B]Gegen Vorratsspeicherung von Telekommunikationsdaten[/B]

Bremen (NRhZ/ILMR, 22.1.) 27 Verbände lehnen in einer heute veröffentlichten Gemeinsamen Erklärung einen Gesetzentwurf von Bundesjustizministerin Brigitte Zypries ab, dem zufolge künftig Daten über jede Nutzung von Telefon, Handy, E-Mail und Internet auf Vorrat gesammelt werden sollen (sog. "Vorratsdatenspeicherung"), damit sie Polizei und Staatsanwaltschaften zur Verfügung stehen. Die Verbände, unter ihnen die Internationale Liga für Menschenrechte, bezeichnen es als "inakzeptabel", dass ohne jeden Verdacht einer Straftat sensible Informationen über die sozialen Beziehungen, die Bewegungen und die individuelle Lebenssituation von über 80 Millionen Bundesbürgerinnen und Bundesbürgern gesammelt werden sollen. Getragen wird die Gemeinsame Erklärung von Bürgerrechts-, Datenschutz- und Menschenrechtsverbänden, von Journalistenorganisationen und Medienverbänden, von der Internetwirtschaft und der Telefonseelsorge, von Anwalts- und Juristenverbänden sowie von der Verbraucherzentrale. Ansprechpartner u.a. Patrick Breyer, Arbeitskreis Vorratsdatenspeicherung, Tel. 0170/5190598, Dr. Rolf Gössner, Internationale Liga für Menschenrechte (ILMR) e.V., Tel. 0421/703354

http://www.nrhz.de/flyer/suche.php?ressort_id_menu=-1&ressort_menu=News

MAUS - 29.1.2007 um 13:36

[B]28.01.2007 07:02

Transfer von EU-Polizeidaten in Drittstaaten soll nicht reguliert werden [/B]

Die deutsche EU-Ratspräsidentschaft hat die EU-Kommission aufgefordert, einen neuen Entwurf für einen Rahmenbeschluss des Ministergremiums zum Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit vorzulegen. Dies geht aus einem Ratsdokument (PDF-Datei) hervor, das die britische Bürgerrechtsvereinigung Statewatch veröffentlicht hat. Zuvor hatte die zivilgesellschaftliche Organisation befürchtet, dass die Bundesregierung den bereits an sich "schwachen" Vorstoß zum besseren Schutz sensibler Polizeidaten komplett unter den Tisch fallen lassen und durch die weniger weitgehenden Datenschutzregeln aus dem umstrittenen Vertrag von Prüm zur stärkeren Vernetzung der EU-Strafverfolgungsbehörden ersetzen wolle.

Einher mit der Forderung nach einem Neustart geht das Eingeständnis, dass das bisherige Verfahren zum Festzurren des Rahmenbeschlusses in eine Sackgasse geraten ist. Der ursprüngliche Entwurf der Kommission vom Herbst 2005 stieß auf Kritik aus vielerlei Richtungen, sodass sich die EU-Gremien im vergangenen Sommer in heftige Auseinandersetzungen verstrickt hatten. Justizkommissar Franco Frattini wollte mit seinem Vorschlag sicherstellen, "dass die personenbezogenen Daten der Bürger mit Sorgfalt und Vorsicht" im Ermittlungsalltag gehandhabt werden. Der Entwurf war auch als kleines Korrektiv für die im Februar vom Rat abgesegnete Richtlinie zur Vorratsspeicherung von Telefon- und Internetdaten gedacht, durch die das elektronische Leben der 450 Millionen EU-Bürger verdachtsunabhängig überwacht werden soll.

Als einer der Hauptstreitpunkte entwickelte sich die Frage, inwieweit beim Transfer von Daten der Sicherheitsbehörden in Drittstaaten dort EU-adäquate Datenschutzregelungen gegeben sein müssen. Der europäische Datenschutzbeauftragte Peter Hustinx pochte mit Unterstützung der europäischen Datenschutzkonferenz gleich zwei Mal in Stellungnahmen darauf, dass hier in allen am Informationsaustausch beteiligten Ländern entsprechende Schutzstandards gegeben sein müssten. Das EU-Parlament vertrat ebenfalls diese Ansicht. Vertreter der US-Regierung

machten dagegen ihr Missfallen über die Drittstaatenregelung deutlich. Washington geht es etwa darum, die auf Basis der Pflicht zur Vorratsdatenspeicherung gesammelten Daten auch für ihre Behörden nutzen zu dürfen.

Die deutsche Ratspräsidentschaft drängt nun darauf, dass es den Mitgliedsstaaten selbst überlassen bleiben soll, inwiefern sie Informationen aus dem Strafverfolgungsbereich mit Drittstaaten teilen. Vor allem bereits bestehende Verträge zum internationalen Datenaustausch dürften durch den Rahmenbeschluss nicht berührt werden. Darüber hinaus listet die Bundesregierung 15 Punkte auf, bei denen ihr eine Einigung auf EU-Ebene leichter zu erreichen scheint. So sollte das Gesetz etwa spezielle Bestimmungen über die Verarbeitung besonders sensibler Daten wie Informationen über Rasse oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gesundheit oder Sexualität enthalten. Zu Verankern seien ferner ein Recht auf Einsicht, Korrektur und Schadensersatz sowie technische und organisatorische Vorschriften zum Schutz gegen unautorisierten Zugriff mit entsprechenden Kontrollpflichten.

Tony Bunyan von Statewatch hofft dagegen, dass die Kommission bei der Neufassung des Entwurfs "nicht nur die Ansichten des Rates, sondern auch die des Europäischen Datenschutzbeauftragten und des Parlaments berücksichtigt." Im Gremium der Mitgliedsstaaten sollte das Vorhaben zudem nicht von der Arbeitsgruppe der Strafverfolger, sondern der Abteilung für Datenschutz beackert werden. Andernfalls könnten die Belange der Ermittler nicht in eine angemessene Balance mit den Bürgerrechten gebracht werden. (Stefan Krempel) / (jk/c't)

<http://www.heise.de/newsticker/meldung/84379>

[B]29.01.2007 11:44

Bundesdatenschutzler warnt vor Überwachungsgesellschaft [/B]

Der Bundesdatenschutzbeauftragte Peter Schaar hat vor einem Missbrauch bei der geplanten vorsorglichen Speicherung von Kommunikationsverbindungsdaten gewarnt. "Ich sehe die von der Bundesregierung geplante Vorratsdatenspeicherung sehr kritisch, mit der Unternehmen verpflichtet werden sollen, Telefon-, Handy- oder Internetdaten über sechs Monate vorzuhalten", sagte Schaar der Tageszeitung Die Welt.

Falls die Politik den Schutz personenbezogener Daten nicht verbessert, sieht Schaar Deutschland "auf dem Weg in eine Überwachungsgesellschaft, die zunehmend von Kontrollen geprägt ist". Es sei das erste Mal, dass "auf so breiter Basis die Daten von völlig unverdächtigen Personen" gespeichert würden – "und zwar nur, damit die Sicherheitsbehörden im Falle strafrechtlicher Ermittlungen darauf zurückgreifen können. Damit ist der Grundsatz der Verhältnismäßigkeit verletzt. Und es bestehen Risiken des Missbrauchs und der Verwendung der Daten für andere Zwecke", kommentierte Schaar die Pläne der Bundesregierung und der EU.

Der Gesetzentwurf von Bundesjustizministerin Brigitte Zypries (SPD) zur Vorratsspeicherung sämtlicher Verbindungs- und Standortdaten, die bei der Abwicklung von Diensten wie Telefonieren, E-Mails, SMS-Versand oder Voice-over-IP-Nutzung anfallen, setzt eine EU-Richtlinie um. Ziel ist es, die Strafverfolgung und den Kampf gegen den Terrorismus zu verbessern, heißt es unisono aus Brüssel und aus Berlin. Verleger- und Wirtschaftsverbände, Journalistengewerkschaften, Datenschützer, Anwälte und Richter hatten die geplante Speicherung als Eingriff in die Privatsphäre und vertrauliche Information bereits heftig kritisiert. Schaars Landeskollege aus Sachsen-Anhalt hatte bereits vor einigen Tagen kommentiert: "Wir leben nicht in einem Überwachungsstaat. Aber die Tendenz zu einer Überwachungsgesellschaft ist unverkennbar."

Es gehe aber bei der Vorratsdatenspeicherung "längst nicht mehr nur um Terrorismusbekämpfung", kritisierte Schaar, sondern auch um handfeste Wirtschaftsinteressen: "Die Musikindustrie zum Beispiel will die gespeicherten Verbindungsdaten, die dem Fernmeldegeheimnis unterliegen, ebenfalls nutzen, um dem Verdacht auf Urheberrechtsverletzungen nachgehen zu können." Es gebe aber unter den Bürgern eine "deutlich gestiegene Sensibilität gegenüber dem Umgang mit den riesigen Datenmengen". Dem müsse Rechnung getragen werden. Diese Einschätzung Schaars dürften die Grünen teilen: Die innenpolitische Sprecherin der Grünen im Bundestag, Silke Stokar, will unter den Bürgern einen sich abzeichnenden Gesinnungswandel rund um den Schutz der Privatsphäre entdeckt haben: "Viele sagen, das geht mir jetzt allmählich zu weit."

<http://www.heise.de/newsticker/meldung/84406>

MAUS - 30.1.2007 um 17:00

[B]29.01.2007 17:57

Hüllenlose Überwachung [/B]

Mit insgesamt mehr als vier Millionen Überwachungskameras zählt Großbritannien bereits heute zu den weltweit führenden Überwachungsgesellschaften. Der durchschnittliche Brite wird jeden Tag rund dreihundert Mal von einer Überwachungskamera gefilmt – und künftig will ihm der Staat offenbar auch unter die Wäsche schauen. Die Tageszeitung The Sun zitiert am heutigen Montag aus internen Papieren, aus denen hervorgeht, dass das britische Innenministerium den flächendeckenden Einsatz versteckter Kameras auf Straßen und Plätzen befürwortet, die mit Terahertz-Strahlung arbeiten und die Kleidung von Passanten durchdringen können.

Eingesetzt werden solche Durchleuchtungssysteme bereits an Flughäfen oder auch von der britischen Polizei, die damit beispielsweise bei Razzien im Londoner Nachtleben nach am Körper versteckten Drogen sucht. Unauffällig in Laternen eingebaut, könnten solche Kamerasysteme vor allem die Suche nach Waffen und Sprengstoffen erleichtern, halten die Verfasser des Berichts fest. Vorbehalte der Bürger gegen heimliche Nacktaufnahmen wollen sie unter anderem damit entgegen, dass Aufnahmen von Frauen nur durch weibliche Sicherheitsmitarbeiter gesichtet werden dürfen – was bei der Beobachtung von Plätzen technisch aber wohl kaum machbar sein dürfte.

Entwickelt werden die Personen-Scanner unter anderem von QinetiQ, einem aus der britischen Militärforschungsorganisation DERA (Defence Evaluation and Research Agency) hervorgegangenen Unternehmen, das seit Februar 2006 an der Londoner Börse gelistet ist und an dem das britische Verteidigungsministerium noch einen Anteil von knapp 20 Prozent hält. Im Programm hat QinetiQ auch Produkte zur Gesichtserkennung, zur automatischen Kennzeichenerfassung sowie Bewegungserkennungs-Software. Mit Militärtechnik- und Big-Brother-Produkten erzielte das Unternehmen im Geschäftsjahr 2005/06 (Ende: 31. März) einen Gewinn vor Steuern in Höhe von rund 121 Millionen Euro. (pmz/c't)

<http://www.heise.de/newsticker/meldung/84454>

[B]30.01.2007 08:38

Schäuble: BiometriePässe stärken den Datenschutz [/B]

Bei einer Diskussionsrunde über den Schutz der Freiheit durch den Staat im Rahmen des ersten europäischen Datenschutztages prallten die Meinungen von Koalitionspolitikern und den Hütern der Privatsphäre in der Landesvertretung Sachsen-Anhalt in Berlin am Montagabend frontal aufeinander. "Ob man etwas zu verbergen hat oder nicht, darauf kommt es nicht mehr an, wenn der Präventionsstaat alle Daten abgreift", beklagte der sachsen-anhaltinische Landesdatenschutzbeauftragte Harald von Bose. So könne der Generalverdacht Alltag werden mit gravierenden Auswirkungen auf die Ausübung der Grundrechte. Bundesinnenminister Wolfgang Schäuble warf dem Datenschützer daraufhin vor, "Unsinn" zu reden. Natürlich müsse das Grundrecht auf informationelle Selbstbestimmung genauso geschützt werden wie jedes andere auch. Es gebe aber "ein zunehmendes Spannungsverhältnis mit der Sicherheit".

Insgesamt muss der Staat dem CDU-Politiker zufolge "in der Lage sein, auf neue Herausforderungen in angemessener Weise zu reagieren". Als Beispiel brachte er die Notwendigkeit im Rahmen der Globalisierung, die "Fälschungssicherheit von Ausweisdokumenten" durch die Integration biometrischer Merkmale wie dem digitalen Gesichtsbild und Fingerabdrücken zu erhöhen. Die von Datenschützern skeptisch beäugte Maßnahme kommt für ihn auch einer "Vorkehr gegen schwerwiegende Verstöße gegen Grundrechte" wie den sich gerade online bietenden Möglichkeiten des Identitätsdiebstahls gleich. "Mit Hilfe moderner Techniken ist auf dem Wege zu gewährleisten, was wir gemeinsam wollen", wischte Schäuble Bedenken gegen eine zunehmende Kontrolle durch ID-Management weg.

Sein Verständnis von Datenschutz umschrieb der Innenminister mit dem Erfordernis der gesetzgeberischen Festlegung, "wer darf Daten zu welchen Zwecken unter welchen Voraussetzungen nutzen und wie lange müssen sie gespeichert werden". Es könne nicht angehen, den Staat "blind" zu machen. Vielmehr sei eine "Datenverkehrsordnung" erforderlich, die einen optimalen Informationsfluss gewährleiste und die "notwendige Datenverarbeitung" transparent mache. Dabei müsse man aus Fehlern Erkenntnisse ziehen. So sprach sich der Minister etwa dafür aus, die von der Union mit beschlossene Eingrenzung der Verwendung der Mautdaten auf Abrechnungszwecke aufzuheben: "Wir sollten eine Grundlage schaffen, die Daten zu nutzen, um Mörder zu erkennen." Alles andere könne man der Bevölkerung nicht erklären.

Konform mit Schäuble ging Dieter Wiefelspütz, Innenexperte der SPD-Fraktion im Bundestag. Er erklärte am Beispiel der von seinem Koalitionskollegen befürworteten Möglichkeit zur "Online-Durchsuchung" von Festplatten privater PCs, dass

es dazu gegenwärtig keine angemessene Rechtsgrundlage gebe. Er sei aber dafür, "dass man da ran kann, wenn es wichtige Gründe gibt". Daher müsse man darüber diskutieren, "was denn da eigentlich so privat ist" im Online-Bereich und "was das Schlafzimmer im Internet" sei. Es könne nicht sein, dass "wir wunderbare technische neue Welten schaffen und die Sicherheit hinterherhinkt".

Allgemein ist Wiefelspütz der Ansicht, dass "wir bei der Volkszählung eine überzogene Diskussion hatten", während sich heute "bis auf die Profis" kaum mehr jemand für den Datenschutz interessiere. Die Bürger würden ihn gerade im Internet "laxer" handhaben. Andererseits gebe es "ungleich größere Gefahren, die zu beherrschen sind", deutete der SPD-Politiker die Möglichkeit eines terroristischen Anschlags auf ein Atomkraftwerk an. Die Polizei arbeite daher inzwischen "viel, viel stärker im Vorfeld", wobei man aber verhindern müsse, "dass das dann uferlos wird". Zum Glück gebe es in Deutschland noch keine Sicherheitshysterie. So etwas wie einen Überwachungsstaat, betonte Wiefelspütz, "haben wir nicht einmal ansatzweise".

Die Bundesverfassungsrichterin Christine Hohmann-Dennhardt monierte dagegen, dass die rechtsstaatlichen Grundsätze "ein wenig zu kurz kommen", gerade wenn Politiker "schon im vorbeugenden Bereich Verbrechen bekämpfen wollen" und entsprechende Befugnisse "immer weiter nach vorne bringen in Vorvorfeld-Situationen". Es werde schwierig mit der Verhältnismäßigkeit, wenn der Mensch "zur reinen Erkenntnisquelle" werde. Konkret wies sie in diesem Zusammenhang etwa auf das "Zusammenspiel von Bund und Ländern hin", das zu der von Karlsruhe als verfassungswidrig beanstandeten Rasterfahndung nach "Schläfern" nach dem 11. September 2001 geführt habe, sowie auf neue Polizeigesetze der Länder mit Normen zum Datenabgleich zur Ermittlung eines reinen Verdachts. Der Staat habe zwar die Freiheit bei "Leib, Leben und vergleichbarem Mehr" zu garantieren. Es gebe aber nicht nur "Sicherheit durch den Staat, sondern auch vor dem Staat."

Von Bose hatte zuvor kritisiert, dass der Staat bei Sicherheitsgesetzen "kaum ein Innehalten und keine Tabus mehr im Hinblick auf seine Grundsätze kennt". Beispiele auf EU-Ebene für diese Praxis brachte der Frankfurter Rechtsprofessor Spiros Simitis. Er nannte unter anderem das Abkommen zur Weitergabe von Flugpassagierdaten (Passenger Name Records, PNR) zwischen Brüssel und Washington. Bei dem schon von der Intention her verfehlten Vertrag habe die EU-Kommission sich zuletzt "wie selbstverständlich damit abgefunden", dass die US-Sicherheitsbehörden entgegen der Vorgaben des Abkommens auf Basis der Daten eine vollautomatisierte Risikoanalyse von Einreisenden treffen würden. In der Affäre um den Finanzdatentransfer durch das SWIFT-Netzwerk sei die Brüsseler Behörde "durch ein Höchstmaß an Passivität aufgefallen". Bei der Vorratsspeicherung von Telefon- und Internetdaten habe sie "eine ihr eindeutig nicht zustehende Kompetenz usurpiert". Mit dem Umsetzungsgesetz aus dem Bundesjustizministerium sei nun endgültig "jede Grenze zur Verfassungswidrigkeit deutlich überschritten".

An die Politik richtete Simitis die Frage, ob sie in einer Zeit, in der "alle Daten vorhanden sind" und man "alles" über einen Menschen in Erfahrung bringen könne, überhaupt noch eine Beschränkung der Informationsverarbeitung auf bestimmte Zwecke akzeptiere. Er plädierte für "Kompensationen" für die fortlaufenden Bürgerrechtseinschnitte wie "klare Fristen, eine spätere Vernichtung der Daten, ein Höchstmaß an Transparenz und eine konsequente Überprüfung der Gesetzgebung."

Der EU-Abgeordnete Alexander Alvaro (FDP) und der Bundesdatenschutzbeauftragte Peter Schaar waren sich einig, dass eine kritische Bestandsaufnahme der in den vergangenen fünf Jahren eingeführten Überwachungsmaßnahmen überfällig sei und diese in der Gesamtschau zu betrachten seien. Angesichts beispielsweise einer verstärkten Videoüberwachung, angesichts ausgebauter DNA-Analyse und angesichts Konten- und Telekommunikationsüberwachung sprächen Verfassungsrichter korrekterweise von einem "additiven Grundrechtseingriff", gab Alvaro zu bedenken. Laut Schaar ist es "an der Zeit, wieder den Vorwärtsgang einzulegen und die Modernisierung des Datenschutzes anzugehen". Die gegenwärtige Situation erinnert ihn ein wenig an die Zeit kurz vor dem Volkszählungsurteil in den Achtzigern, als das informationelle Selbstbestimmungsrecht im Grundgesetz verankert wurde. Die Politik müsse "wieder durchgerüttelt werden" und sollte "mehr Phantasie auch im Hinblick auf den Schutz der Bürgerrechte" entwickeln. (Stefan Krempel) / (jk/c't)

<http://www.heise.de/newsticker/meldung/84463>

MAUS - 4.2.2007 um 15:51

[B]02.02.2007 15:51

Bundesgerichtshof entscheidet über Online-Durchsuchungen [/B]

Der Bundesgerichtshof (BGH) entscheidet am Montag, ob die Polizei Computer heimlich online durchsuchen darf, gab das Karlsruher Gericht am heutigen Freitag laut dpa bekannt. Mit dem Beschluss will der BGH klären, ob die bisherigen

gesetzlichen Grundlagen für Online-Durchsuchungen ausreichen. Ein BGH-Ermittlungsrichter hatte dies im Februar des vergangenen Jahres bejaht, ein anderer Ermittlungsrichter hatte dagegen im November das heimliche Ausforschen von Computerfestplatten für unzulässig erklärt. Die Bundesanwaltschaft hat Beschwerde eingelegt, so dann nun der 3. Strafsenat eine abschließende Entscheidung fällen muss.

BGH-Ermittlungsrichter Ulrich Hebenstreit hatte eine Anwendung der Vorschrift über die Hausdurchsuchung schon deshalb abgelehnt, weil diese offen und in Anwesenheit des Betroffenen stattfindet, während das Ausspähen von Daten mithilfe eines Trojaners heimlich vor sich geht. Er verglich solche Maßnahmen mit dem großen Lauschangriff, weil die auf einem Computer gespeicherten Daten oft ähnlich sensibel seien wie eine vertrauliche Unterhaltung in den eigenen vier Wänden. Angesichts der Datenfülle könne der Betroffene zudem zum "gläsernen Menschen" werden; gespeicherte Dateien könnten mitunter auch Tagebuchqualität haben. Ein derart gravierender Eingriff in die Rechte Betroffener könne nicht ohne eigenständige gesetzliche Grundlage angeordnet werden, argumentierte der Richter.

Die Entscheidung ist politisch brisant, weil das Bundesinnenministerium erst vor kurzem die technischen Voraussetzungen für Online-Durchsuchungen beim Bundeskriminalamt verbessern wollte. Damit sollten nach Ansicht von Bundesinnenminister Wolfgang Schäuble unter anderem die Aufklärung möglicher Terrorplanungen verbessert werden. Wenn der BGH die Vorschriften der Strafprozessordnung als nicht ausreichend einstuft, müsste dafür zunächst eine Regelung geschaffen werden.

Im nordrhein-westfälischen Verfassungsschutzgesetz ist die Möglichkeit zur Online-Durchsuchung bereits seit kurzem festgehalten; dagegen ist aber eine Verfassungsklage in Vorbereitung. Schäuble hatte die Möglichkeit für einen "Bundestrojaner" in seinem 132 Millionen Euro schweren Programm zur Stärkung der inneren Sicherheit anfangs nur angedeutet. Als "Bundestrojaner" wird inoffiziell der Teil eines Programmes bezeichnet, der Spyware-Code auf einen PC einschleust, damit eine Online-Durchsuchung durch die Strafverfolgungsbehörden oder Geheimdienste möglich wird. Auf eine Anfrage der Grünen hatte das Bundesinnenministerium dann Anfang Januar mitgeteilt, dass für die Programmierung der Software zwei Programmierstellen notwendig seien, die teils aus laufenden Mitteln, teils von Mitteln aus dem Programm zur Stärkung der Inneren Sicherheit bezahlt werden. Insgesamt soll das Tool zur Online-Durchsuchung nicht mehr als 200.000 Euro kosten.

Unterstützung bekam Schäuble vor kurzem vom Dieter Wiefelspütz, Innenexperte der SPD-Fraktion im Bundestag. Er ist zwar der Ansicht, dass für die "Online-Durchsuchung" gegenwärtig keine angemessene Rechtsgrundlage gebe. Wiefelspütz sprach sich aber dafür aus, "dass man da ran kann, wenn es wichtige Gründe gibt". Daher müsse man darüber diskutieren, "was denn da eigentlich so privat ist" im Online-Bereich und "was das Schlafzimmer im Internet" sei. Es könne nicht sein, dass "wir wunderbare technische neue Welten schaffen und die Sicherheit hinterherhinkt". Neben den datenschutzrechtlichen Aspekten und den Erwägungen über Verletzung der Grundrechte kommen in der politischen Diskussion die technischen Unwägbarkeiten und die mögliche Unwirksamkeit eines Bundestrojaners, die sich angesichts der heutzutage gegen kriminelle Machenschaften von Viren- und Trojanerschreibern sowie Botnetzbetreibern empfohlenen Schutzmaßnahmen für Internetnutzer ergeben, kaum vor. Für den Bundesgerichtshof zumal dürften diese Fragen aus grundsätzlichen Überlegungen heraus keine Rolle spielen.

<http://www.heise.de/newsticker/meldung/84726>

[B]03.02.2007 14:40

Harsche Kritik an Online-Durchsuchungen [/B]

Ex-Bundestagsvizepräsident Burkhard Hirsch (FDP) hält die heimliche Online-Durchsuchung von Computern durch die Polizei für "schlimmer als den Großen Lauschangriff", meldet das Nachrichtenmagazin Der Spiegel in seiner kommenden Ausgabe. Das Ausspähen des Privatcomputers per Internet – etwa auf der Basis eines "Kommissar Trojaner" nach Schweizer Vorbild – sei ein "brutalerer Eingriff" als alle bisherigen Ermittlungsmethoden: "Der PC ist ja wie ein ausgelagertes Gehirn."

Am Montag gibt der Bundesgerichtshof (BGH) bekannt, ob er verdeckte Online-Durchsuchungen in Strafverfahren bereits auf der Grundlage bestehender Gesetze für möglich hält. Gegen ein nordrhein-westfälisches Gesetz, das dies auf Landesebene legalisieren will, haben Bürgerrechtler bereits Verfassungsbeschwerde angekündigt. Hirsch hält solche Überwachungen per "Computerwanze" allenfalls für zulässig, "wenn dabei mindestens derselbe Schutz für den Kernbereich privater Lebensgestaltung greift wie beim Großen Lauschangriff". Bei der akustischen Wohnraumüberwachung hatte Hirsch mit einer erfolgreichen Verfassungsbeschwerde drastische Einschränkungen durchgesetzt. (gr/c't)

<http://www.heise.de/newsticker/meldung/84748>

MAUS - 4.2.2007 um 16:03

[B]02.02.2007 15:18

Bundestag streitet über Aufnahme von Fingerabdrücken in Reisepässe [/B]

Der Bundestag hat in der Nacht zum heutigen Freitag in 1. Lesung über den Regierungsentwurf zur Änderung des Passgesetzes beraten, den das Bundeskabinett Ende Dezember vergangenen Jahres beschloss und mit dem die Speicherung von zwei Fingerabdrücken zusätzlich zum Lichtbild möglich werden soll. "Die Technik kann einen wichtigen Beitrag für die innere Sicherheit leisten", begründete Peter Altmaier (CDU), parlamentarischer Staatssekretär beim Bundesinnenministerium, den Vorstoß. Zugleich werde eine entsprechende EU-Verordnung umgesetzt.

Oppositionspolitiker lehnten die Initiative aber als weiteren Schritt in den Überwachungsstaat ab. Sie führten unisono allgemeine Datenschutz- und Sicherheitsbedenken hauptsächlich rund um den RFID-Funkchip ins Feld, auf dem künftig neben dem Gesichtsbild auch die Fingerabdrücke gespeichert werden sollen. Auch bei der SPD sorgte zudem die Tatsache für Empörung, dass die Lesung in die frühen Morgenstunden gelegt worden war, die Reden somit zu Protokoll gegeben werden mussten und eine echte Debatte vermieden wurde.

"Mit der Einführung der digitalen Gesichtsbilder hat Deutschland einen gigantischen Feldversuch für die Biometrietechnik gestartet, und das ohne jeden Probelauf", erklärte Gisela Piltz, Innenexpertin der FDP-Fraktion. "Es schadet aber der Demokratie, wenn eine gesellschaftliche Auseinandersetzung über die Herrschaft der Menschen über ihre biometrischen Daten nicht stattfindet." Es gehe schließlich um die "elementarsten", den "höchstpersönlichsten Lebensbereich" betreffenden menschlichen Informationen, die etwa auch Auskunft über Erbkrankheiten, Abstammung oder Verwandtschaft geben könnten. Deutschland dürfe daher nicht blind "Vorreiter einer neuen biometrischen Überwachungswelle" werden. Zugleich kritisierte die Liberale, dass das Innenministerium die wahren Kosten der elektronischen Ausweisdokumente etwa über das Verschweigen von Personalmehraufwand verschleierte und der Bundesdruckerei allein ein gutes Geschäft zuchustere.

Gemeinsam mit ihrem Kollegen von den Linken, Jan Korte, betonte Piltz, dass die geplante Änderung mit anderen Gesetzesvorhaben wie der Einführung biometrischer Merkmale auch in den Personalausweis oder der fortschreitenden Vernetzung von Polizeidaten im Schengen-Raum und darüber hinaus zu sehen sei. In diesem Rahmen würden die Motive für die Biometrie-Offensive deutlicher. So verwiesen die beiden Oppositionspolitiker insbesondere auf eine Klausel im Regierungsentwurf des Gesetzes über die Aufrüstung des Personalausweises, wonach "im Falle der Übermittlung von Lichtbildern an die Polizei- und Ordnungsbehörden im Rahmen der Verfolgung von Verkehrsordnungswidrigkeiten der Abruf des Lichtbildes im automatisierten Verfahren erfolgen kann". Dies eröffne letztlich in Kombination mit der ebenfalls intensiv betriebenen Ausweitung der Videoüberwachung ganz neue Möglichkeiten für die Strafverfolgung, fürchtete Piltz. Korte monierte die eindeutige Missachtung der Zweckbindung der biometrischen Daten, wenn diese plötzlich auch zur Klärung von Bußgeldverfahren herangezogen werden könnten.

Innenminister Wolfgang Schäuble, der die elektronischen Ausweisdokumente jüngst als Mittel zur Stärkung des Datenschutzes in der Online-Welt anpries, pflegt laut Korte "auch mit dem neuen Passgesetz seine Datensammelobsession." Die biometrischen Daten fast aller Bundesbürger würden "auf Vorrat gespeichert und in einer Referenzdatei zusammengeführt". Dabei handle es sich letztlich um nichts anderes "als die Einführung einer universellen Personenkennziffer durch die Hintertüre."

In die gleiche Kerbe schlug Wolfgang Wieland, innenpolitischer Sprecher der Grünen, der an die geplante Zentralisierung der Melderegister erinnerte und vor einer Orwellschen Gesetzgebung warnte. "Wenn man die Angaben über den Wohnort und die dort eingegebenen Lichtbilder mit der Datei verbindet, dann haben Sie die Datei, die Ihnen die totale Überwachung der Bürger ermöglicht." Der Fingerabdruck sei zudem keineswegs fälschungssicher und entsprechende Biometriesysteme könnten mit einfachsten Mitteln ausgetrickst werden, wie es etwa der Chaos Computer Club (CCC) wiederholt vorgeführt habe. Ferner sei die Aufnahme der Fingerabdrücke europarechtlich nicht erforderlich, da dies in den Brüsseler Vorgaben als reine "Soll-Verordnung" ausgeführt worden sei.

In der Richtung unentschlossen zeigte sich Frank Hofmann von der SPD, in deren linken Flügel es starke Bedenken gegen biometrische Ausweisdokumente gibt. "Weder sicherheitspolitisch sinnvolle Maßnahmen noch terroristische Bedrohungsszenarien" dürfen seiner Ansicht nach "den wesentlichen Blick auf den Schutz der bürgerlichen Freiheiten und Grundrechte verstellen." Dabei müsse das fragile Gleichgewicht zwischen Freiheit und Sicherheit immer wieder austariert werden. Zu diesem öffentlichen Prozess gehöre auch, "dass wir uns als nationaler Gesetzgeber sicherheitspolitische Notwendigkeiten nicht von europäischen Ratsverordnungen diktieren lassen".

Zugleich räumte der Sozialdemokrat ein, dass die im Raum stehenden Änderungen bei der Verfolgung von Straßenverkehrsordnungswidrigkeiten eine der "kleineren Schwächen" der Gesetzesvorhaben darstelle. "Wenn man solche Maßnahmen in Sicherheitsgesetzen verankert, dann macht man es den Gegnern leicht in ihrer Argumentation, es ginge vermehrt um die Kriminalisierung und Bestrafung unbescholtener Bürger", schalt Hofmann die Bundesregierung indirekt. Man müsse sich ferner "bewusst machen, dass die erstmalige Erhebung von Fingerabdrücken zur Identifizierung in Personaldokumenten in der Bevölkerung mit der erkennungsdienstlichen Behandlung von Kriminellen verknüpft werden könnte". Trotz Datenschutz dürfe sich die Koalition aber vor "technischen Innovationen" nicht verschließen. Durch biometrische Merkmale im Pass werde es möglich, "die Identität von Personen, vor allem bei Grenzkontrollen, durch Vergleich mit den Merkmalen der kontrollierten Person festzustellen." Man werde daher bei der weiteren Beratung des Gesetzesentwurfs an der SPD-Maxime "Sicherheitspolitik mit Augenmaß" festhalten.

<http://www.heise.de/newsticker/meldung/84725>

MAUS - 12.2.2007 um 16:38

08.02.2007 19:44

[B]Schäuble: Trojaner sollen auch private Tagebücher durchsuchen [/B]

In einem Interview mit der taz hat Bundesinnenminister Wolfgang Schäuble (CDU) bekräftigt, dass es bei der geplanten verdeckten Online-Durchsuchung keine privaten Bereiche auf der Computerfestplatte geben kann, die im Sinne des "Kernbereichs privater Lebensführung" geschützt sind. Damit bezieht Schäuble in der aktuellen Debatte um Online-Durchsuchungen einen deutlichen Gegenpol zu Bundesjustizministerin Brigitte Zypries (SPD). Sie hatte vor Schnellschüssen gewarnt und ergänzend erklärt, das man genau überlegen müsse, welche Folgen ein so erheblicher Eingriff in die Privatsphäre haben könnte.

Im taz-Interview wurde Schäuble gefragt, wie er zum Kernbereich "private Lebensführung" stehe, dessen Schutz vom Bundesverfassungsgericht mehrfach angemahnt wurde. Schäubles Antwort im Wortlaut: "Ich kenne und respektiere die Rechtsprechung des Bundesverfassungsgerichts zum Schutz der Privatsphäre. Aber wir müssen auch sehen, dass dieser Schutz in der Alltagswirklichkeit praktikabel bleibt. Verbrecher und Terroristen sind klug genug, so etwas auszunutzen. Die tarnen ihre Informationen dann zum Beispiel als Tagebucheintrag. So leicht dürfen wir es denen nicht machen."

Wenn terroristische Details in Tagebucheinträgen, Liebesbriefen oder Steuererklärungen stecken können, kann es Schäuble zufolge keine Einschränkung durch private Bereiche geben. Entsprechend kündigte er im Interview eine Prüfung an, ob für den Einsatz des "Bundestrojaners" eine Verfassungsänderung nötig sei.

"An das Internet muss er aber immer", ist laut Innenminister die eindeutige Lehre, die Strafverfolger aus dem bisherigen Verhalten von Terroristen geschlossen haben. Dementsprechend müssten ihnen Trojaner geschickt werden, von denen Schäuble zugibt, "gerade mal so" zu wissen, was die Trojaner können. Er selbst habe jedoch keine Angst vor Spionage-Software, so Schäuble im Interview: "Nein, ich öffne grundsätzlich keine Anhänge von E-Mails, die ich nicht genau einschätzen kann. Außerdem bin ich anständig, mir muss das BKA keine Trojaner schicken."

Befragt, warum er denn Ende 2004 dem Mautgesetz zugestimmt habe, das die Verwendung von Mautdaten für Fahndungszwecke ausdrücklich verbietet, erklärte Schäuble sein damaliges Abstimmungsverhalten als schweren Fehler. "Von mir hören Sie keine Versprechungen mehr, dass alles so bleibt wie es ist."

<http://www.heise.de/newsticker/meldung/85023>

09.02.2007 14:24

[B]Verfassungsbeschwerde gegen Online-Durchsuchungen in NRW eingelegt [/B]

Der Berliner Rechtsanwalt Fredrik Roggan hat am heutigen Freitag im Auftrag der Mülheimer Autorin Bettina Winseman (alias Twister) und einem Mitglied der Linkspartei das Bundesverfassungsgericht wegen des neuen nordrhein-westfälischen Verfassungsschutzgesetzes angerufen. Die Beschwerde richtet sich gegen die in diesem Gesetz erstmals offiziell eingeführten heimlichen Online-Durchsuchungen von Computern durch Sicherheitsbehörden, die Bundesinnenminister Wolfgang Schäuble (CDU) bundesweit auf eine gesetzliche Grundlage stellen will.

In NRW darf der Verfassungsschutz seit dem 20. Dezember Computer, die mit dem Internet verbunden sind, heimlich

ausspähen. Dabei sollen die auf einem Rechner gespeicherten Dateien ohne Kenntnis der Betroffenen durchsucht werden können. "Im Einzelfall hat der Geheimdienst damit Zugriff auf Informationen, die ansonsten nur für die Polizei mit einer Hausdurchsuchung zu erlangen wären", hält Roggan dagegen, der auch stellvertretender Bundesvorsitzender der Bürgerrechtsorganisation Humanistische Union ist: Mit verdeckten Online-Durchsuchungen könne allgemein tief in die Privatsphäre von Personen eingegriffen werden, die – aus welchen Gründen auch immer – in das Visier des Verfassungsschutzes geraten sind. Deshalb sei es möglich, dass die im deutschen Recht gänzlich neue Maßnahme einen Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung darstelle.

Gute Chancen rechnet Roggan der Beschwerde insbesondere aus, da die Befugnis im NRW-Verfassungsschutzgesetz nicht einmal einen Richtervorbehalt vorschaltet. Einen solchen hält der Anwalt für unabdingbar. Das Gesetz sei aber "auf jeden Fall" auch verfassungswidrig, weil es keine Vorkehrungen zum Schutz der Intimsphäre enthalte. "Wer in Nordrhein-Westfalen auf seinem Rechner auch tagebuchartige Aufzeichnungen oder Fotos von nahen Angehörigen speichert, kann nicht mehr sicher sein, dass solche höchstpersönlichen Sachverhalte nicht staatlicherseits heimlich ausgespäht werden können", moniert Roggan.

Ein weiterer Beschwerdepunkt ist die Befugnis des Verfassungsschutzes zur Teilnahme an "Kommunikationseinrichtungen des Internet", also etwa Chatrooms. "Hier wird erstmals gesetzlich eine Mitwirkung des Geheimdienstes an Veranstaltungen, die er seinem Auftrag entsprechend eigentlich nur zu beobachten hätte, zugelassen", listet der Bürgerrechtsanwalt die Fehler des Gesetzes weiter auf. "Dass dies ein Irrweg ist, hat das Bundesverfassungsgericht zuletzt im NPD-Verbotsverfahren herausgestellt." Das Verbot sei daran gescheitert, dass aufgrund der Involvierung von Verfassungsschutzbehörden in die Parteiarbeit nicht ausreichend erkennbar war, ob es sich bei der NPD nicht letztlich um eine "staatliche Veranstaltung" handelte.

Die Mitbeschwerdeführerin Twister sieht durch das Gesetz vor allem ihre Arbeit als Journalistin und ihre Privatsphäre in unzumutbarem Maße gefährdet. Zugleich will sie der Verabschiedung weiterer Gesetze nach Muster der NRW-Regelung zu Online-Durchsuchungen in anderen Bundesländern einen Riegel vorschieben. Nach dem Verbot von heimlichen Online-Durchsuchungen durch den Bundesgerichtshof (BGH) hatte außer Bundesinnenminister Wolfgang Schäuble zunächst das bayerische Kabinett angekündigt, eine Rechtsgrundlage für eine heimliche Online-Durchsuchung von PCs zu prüfen. Damit soll eine vom bayerischen Ministerpräsidenten Edmund Stoiber (CSU) entdeckte "Sicherheitslücke zu Lasten der Bürger" geschlossen werden. Andere Landesregierungen sind sich noch uneins über konkrete Schritte.

<http://www.heise.de/newsticker/meldung/85064>

10.02.2007 00:12

[B]Datenschützer warnt vor schrankenloser Ausforschung durch Online-Durchsuchung [/B]

Der Berliner Datenschutzbeauftragte Alexander Dix hat sich vehement gegen die Schaffung einer Rechtsgrundlage für "Online-Durchsuchungen" ausgesprochen. "Es ist widersinnig, dass Sicherheitsbehörden einerseits zu Recht Schutzmaßnahmen gegen den Einsatz von Spionageprogrammen durch Wirtschaftskriminelle fordern, andererseits aber genau diese Schadprogramme einsetzen wollen", erklärte Dix. Der Einsatz von Trojanern für die heimliche Inspektion von Festplatten vernetzter Computer stelle "stets einen massiven Eingriff in die Privatsphäre der betroffenen Internetnutzer" dar. Da die Durchsuchung für die Betroffenen nicht kontrollierbar erfolge, gäbe es laut Dix "keine technischen Schranken für die umfassende Ausforschung beliebiger Bürger." Der Berliner Datenschützer findet deutliche Worte: "Online-Durchsuchungen schaden der inneren Sicherheit und sind verfassungswidrig!"

Die eingesetzte Technik könnte dem Datenschutzbeauftragten zufolge überdies "immense wirtschaftliche Schäden" anrichten, insofern sie zu Zwecken der Wirtschaftsspionage eingesetzt werden. Dix spricht hier von einem "Einfallstor für Kriminelle". Paradoxerweise habe just das Bundesamt für Verfassungsschutz aber soeben vor den wachsenden Risiken der Ausspähung von Unternehmensgeheimnissen gewarnt, die insbesondere von China, Russland und den USA ausgehen.

Auch der größte Befürworter einer bundesweiten gesetzlichen Regelung für den Einsatz von Malware zur Verbrechensbekämpfung, Bundesinnenminister Wolfgang Schäuble (CDU) weise die Bürger und die deutsche Wirtschaft immer wieder auf Gefahren hin, die vom Einschleusen von Spionageprogramme durch Cyberkriminelle über E-Mails oder Webseiten ausgehen, beschreibt Dix den unausweichlichen Zwiespalt weiter. Das Bundesinnenministerium verfolge eigentlich einen "Nationalen Plan zum Schutz der Informationsinfrastrukturen", der die Stärkung der IT-Sicherheit durch Unternehmen und Verbraucher bezwecke. Dieser ziele unter anderem darauf ab, "dass sich jedermann durch Schutzprogramme vor Spionagewerkzeugen schützt".

Der Bundesgerichtshof (BGH) erklärte Anfang der Woche verdeckte Online-Durchsuchungen durch Strafverfolgungsbehörden für rechtswidrig. Seitdem ist innerhalb der Regierung und der großen Koalition ein heftiger Streit über Sinn und Zweck einer gesetzlichen Regelung der tief in die Privatsphäre eingreifenden Maßnahme und über dafür eventuell erforderliche Verfassungsänderungen entbrannt. Während Vertreter der Sicherheitsbehörden immer wieder betonen, mit dem technischen Fortschritt und den Methoden der Kriminellen Schritt halten zu müssen, sehen Skeptiker wie Bundesjustizministerin Brigitte Zypries (SPD) mit der Festplattenspionage dagegen einen Paradigmenwechsel im deutschen Strafrecht einhergehen und warnen vor Schnellschüssen, die in Karlsruhe keinen Bestand hätten.

Als Testballon gilt derweil das im Dezember vom nordrhein-westfälischen Landtag beschlossene neue Verfassungsschutzgesetz NRW. Es enthält erstmals eine Rechtsgrundlage für Online-Durchsuchungen. Allerdings läuft seit dem Freitag eine Verfassungsbeschwerde in Karlsruhe gegen den Vorstoß. Das Beispiel des nordrhein-westfälischen Gesetzgebers darf Dix zufolge in Deutschland auch keine Schule machen, da die gestatteten Befugnisse der inneren Sicherheit letztlich schaden würden und verfassungswidrig seien.

<http://www.heise.de/newsticker/meldung/85078>

10.02.2007 15:06

[B]Online-Durchsuchungen: Polizei nein, Verfassungsschutz ja [/B]

Der Innenminister von Nordrhein-Westfalen, Ingo Wolf (FDP), lehnt heimliche Online-Durchsuchungen von privaten Computern durch Polizei und Staatsanwaltschaft ab. "Nach derzeitigem Stand sehen wir keine Notwendigkeit", sagte Wolf dem Nachrichtenmagazin Focus. Bundesinnenminister Wolfgang Schäuble (CDU) hatte solche verdeckten Ermittlungen in Computern als "unerlässlich" bezeichnet. Wolf forderte die Bundesregierung auf, überzeugende Gründe für eine Änderung der Strafprozessordnung vorzulegen: "Die Beweislast liegt bei Herrn Schäuble."

Seinem Verfassungsschutz hat Nordrhein-Westfalen dagegen als bisher einziges Bundesland ausdrücklich per Gesetz Online-Durchsuchungen erlaubt. Terroristen hätten sich "über das Internet verständigt und dort ihre Bau-Anleitungen für Bomben abgelegt". Als "Ausnahme-Instrument" müsse dem Verfassungsschutz daher auch die heimliche PC-Suche erlaubt sein, so Wolf.

Politiker von Union und SPD forderten im Focus eine gesetzliche Regelung für den Bundesverfassungsschutz. "Der Staat darf sich nicht dümmer stellen als er ist", sagte der CDU-Rechtsexperte Jürgen Gehb. "Aber jeder Eingriff bedarf einer gesetzlichen Ermächtigung." Der SPD-Innenpolitiker Dieter Wiefelspütz hält Online-Durchsuchungen durch den Verfassungsschutz ebenfalls für erforderlich, aber: "Haben wir ausreichende gesetzliche Grundlagen? Meine Antwort ist nein."

<http://www.heise.de/newsticker/meldung/85101>

MAUS - 20.2.2007 um 15:47

[B]16.02.2007 11:28

BKA-Chef legt nach: Polizei braucht Online-Durchsuchungen dringend [/B]

Nach den Debatten der vergangenen Tage über die heimlichen Online-Durchsuchungen von PCs durch Strafverfolger und Geheimdienste legt BKA-Chef Jörg Ziercke noch einmal nach. Im Interview mit der Tageszeitung Die Welt betonte er, die Polizei brauche dieses Instrument dringend, "um zum Beispiel Terrorismus, organisierte Kriminalität, Menschen- und Waffenhandel besser bekämpfen zu können". Zuletzt hatte Ziercke auf dem 10. europäischen Polizeikongress die aus seiner Sicht dramatischen Folgen dargestellt, die das Urteil des Bundesverfassungsgerichtes zum großen Lauschangriff für die Polizeiarbeit habe: Weil das Gericht einen Kernbereich privater Lebensführung von Abhöraktionen ausgenommen habe, sei das Instrument des Abhörens praktisch unbrauchbar geworden. "Das darf mit der Online-Durchsuchung nicht passieren. Die Polizei muss mit dem technischen Fortschritt der Täter mithalten."

Ziercke forderte nun gegenüber der Zeitung erneut eine gesetzliche Regelung für Online-Durchsuchungen. Dafür spreche die Zustimmung in Teilen der Politik und bei den Bürgern. Nach einer Umfrage seien 64 Prozent der Bevölkerung dafür, dass ein Kompromiss gefunden werde. 24 Prozent sagten, die Polizei solle diese Möglichkeit bekommen. Nur 10 Prozent seien völlig dagegen. Allerdings meinte Ziercke auch, die tatsächliche Bedrohungslage und das Bewusstsein darüber würden auseinander klaffen. "Seit dem Jahr 2000 gab es in Deutschland sechs massive

Anschlagsversuche. Aktuell laufen mehr als 220 Ermittlungsverfahren, fast die Hälfte davon beim BKA. Man kann also nicht so tun, als ob wir nicht bedroht sind."

Verärgert zeigte sich Ziercke über die Aussage von Bundesjustizministerin Brigitte Zypries (SPD), die vor staatlichen Hackern gewarnt habe. "Dann müsste man auch Polizisten, die mit richterlichem Beschluss eine Wohnung durchsuchen, als Einbrecher bezeichnen", sagte er. "Niemand muss Orwellsche Verhältnisse befürchten – 99,99 Prozent der Bevölkerung werden davon nicht betroffen sein." Von der Politik fühle er sich zwar nicht im Stich gelassen, es gebe aber bei der verdeckten Online-Durchsuchung eindeutig einen Dissens.

In ihrer Eröffnungsrede auf dem Polizeikongress hatte Zypries über ihre grundsätzlichen Bedenken hinaus festgestellt, dass der Polizeiberuf in Deutschland höchstes Ansehen genieße und Polizisten gleich nach den Ärzten und Krankenschwestern auf dem dritten Platz der Beliebtheitsskala stünden. Zypries warnte davor, dieses Ansehen durch eine "leichtfertig geführte Diskussion" über die Online-Durchsuchung zu gefährden. Dabei kritisierte sie die "beschönigende Untertreibung", die in der Verwendung des Wortes "Durchsuchung" begründet sei. Tatsächlich handele es sich um einen sehr tiefgreifenden Eingriff in den Kernbereich der privaten Lebensführung.

Der Bundesgerichtshof (BGH) hatte heimliche Online-Durchsuchungen privater und geschäftlich genutzter PCs durch Strafverfolgungsbehörden für rechtswidrig erklärt. Seitdem ist innerhalb der Regierung und der großen Koalition ein heftiger Streit über Sinn und Zweck einer gesetzlichen Regelung der tief in die Privatsphäre eingreifenden Maßnahme und über dafür eventuell erforderliche Verfassungsänderungen entbrannt. Während Vertreter der Sicherheitsbehörden immer wieder betonen, mit dem technischen Fortschritt und den Methoden der Kriminellen Schritt halten zu müssen, sehen Skeptiker mit der Festplattenspionage dagegen einen Paradigmenwechsel im deutschen Strafrecht einhergehen. Zypries hatte bereits vor einigen Tagen vor Schnellschüssen gewarnt, die in Karlsruhe keinen Bestand hätten.

Der Kabinettskollege von Zypries, Bundesinnenminister Schäuble, hat allerdings bereits angekündigt, schnell eine gesetzliche Grundlage schaffen zu wollen, damit heimliche Online-Durchsuchungen durch die Strafverfolgungsbehörden möglich werden; diese Maßnahme sei unverzichtbar. Schäuble (CDU) hatte zudem bekräftigt, dass es bei der geplanten verdeckten Online-Durchsuchung keine privaten Bereiche auf der Computerfestplatte geben könne, die im Sinne des "Kernbereichs privater Lebensführung" geschützt seien.

Ziercke warnte in dem aktuellen Interview aber auch die Wirtschaft vor steigender Internet-Kriminalität. "Rund die Hälfte der deutschen Unternehmen unternimmt viel zu wenig für die Datensicherheit", sagte er. Das Vertrauen ins Internet sei äußerst wichtig, da der Handel über das Netz ein wachsender Wirtschaftsfaktor sei. Im Internet würden in Deutschland derzeit rund 45 Milliarden Euro umgesetzt. "Wir möchten die Täter aus dem Verkehr ziehen, die dieses Vertrauen missbrauchen."

<http://www.heise.de/newsticker/meldung/85416>

[B]17.02.2007 13:54

Baden-Württemberg plant "Videoatlas" von privaten Überwachungskameras [/B]

Vergangenes Jahr hatte Baden-Württembergs Innenminister Heribert Rech (CDU) angekündigt, dass die Polizei auch die "Überwachungskameras privater Betreiber" nutzen soll. Die überwiegende Zahl der Videokameras befinde sich in nicht-öffentlichen Bereichen: „Die Polizei soll sich in einem Einkaufszentrum aufschalten können, wenn da etwas passiert. Und dann möchte ich wissen, wo im Umkreis des Tatortes andere Kameras stehen“, so Rech. Auch bei großen Menschenansammlungen soll die Videoüberwachung möglich sein. Rech hatte angekündigt, dass für die Polizei ein "Atlas" aller Videokameras erstellt und diese eine Kooperationsvereinbarung mit den Betreibern erwirken soll. Als Grund für die Ausdehnung der Videoüberwachung gibt Rech die "Gefahr islamistischer Terroranschläge" an, die Idee dazu war nach den gescheiterten Bombenattentaten im Sommer auf Regionalzüge entstanden.

Für die Erstellung der Übersicht und den Zugriff auf private Kameras müsste allerdings das Polizeigesetz geändert werden, was bislang noch nicht geschehen ist. Die Grünen im Landtag haben Kenntnis darüber erhalten, dass vom Innenministerium bereits Betreiber privater Videokameraanlagen befragt wurden, und protestieren gegen dieses Vorgehen, für das jede rechtliche Grundlage fehle. Der innenpolitische Sprecher der Landtagsgrünen Uli Sckerl spricht von Rechts "Videoatlas-Phantasien". Sie gingen weit über die Beschlüsse der Innenministerkonferenz zur erweiterten Videoüberwachung hinaus: "In Baden-Württemberg will der Minister private Betreiber von Videokameras zum verlängerten Arm der Polizei dort machen, wo diese nicht tätig werden darf."

<http://www.heise.de/newsticker/meldung/85460>

[B]17.02.2007 18:51

Auch Generalbundesanwältin für Regelung zu Online-Durchsuchungen [/B]

Generalbundesanwältin Monika Harms hat die Forderung von Bundesinnenministerium und Polizeibehörden nach einer gesetzlichen Regelung für heimliche Online-Durchsuchungen von PCs unterstützt. "Wir müssen technisch auf Augenhöhe mit den Terroristen bleiben und dürfen nicht nur hinterherhecheln", sagte sie der Tageszeitung Die Welt. Angesichts der rasanten Entwicklung der Internettechnik habe sie die Sorge, dass Deutschland gesetzgeberisch auf Dauer im Hintertreffen bleibe.

Der Bundesgerichtshof (BGH) hatte das heimliche Ausspähen von Festplatten über das Internet aber wegen fehlender Rechtsgrundlage verboten. Bundesinnenminister Wolfgang Schäuble (CDU), Bundeskriminalamts-Chef Jörg Ziercke und andere Polizeivertreter dringen seitdem auf eine gesetzliche Regelung, die den Strafverfolgern und den Geheimdiensten die Online-Durchsuchung von PCs erlaubt. Bundesjustizministerin Brigitte Zypries (SPD) hegt jedoch schwere rechtliche Bedenken und äußerte sich bislang skeptisch, ob dieser Weg etwas bringt.

Harms sagte, an der grundsätzlichen Notwendigkeit heimlicher Ermittlungsmaßnahmen könne es keinen Zweifel geben. "Die haben wir auch im Bereich der Überwachung der Telekommunikation oder bei Observationen. Wir brauchen sie auch, weil diese Ermittlungen, wenn sie öffentlich werden, nutzlos sind." Sie sei sich mit Zypries einig, dass ein solches Gesetz gut durchdacht werden müsse, erklärte Harms. "Wir müssen diese aufgeregte Diskussion auf eine sachliche Ebene bringen und festlegen: Bei welchen Straftaten sind Online-Durchsuchungen erforderlich, und unter welchen Bedingungen dürfen die Ermittlungsbehörden tätig werden?"

Berlins Innensenator Ehrhart Körting (SPD) hat sich dagegen erneut dafür ausgesprochen, vor möglichen aufwendigen Gesetzesänderungen den Effekt heimlicher Online-Durchsuchungen von Computern verdächtiger Personen zu prüfen. Schon jetzt sei es für den PC-Nutzer technisch möglich, den Zugriff auf seine Dateien weitgehend auszuschließen, sagte der Vorsitzende der Innenministerkonferenz in einem dpa-Gespräch. Es müsse also zunächst eine technische Bestandsaufnahme gemacht werden, bevor der Gesetzgeber angerufen wird. Körting hatte bereits auf dem 10. europäischen Polizeikongress in dieser Woche die Pläne zur gesetzlichen Regelung von Online-Durchsuchung mit den Worten kommentiert, mit dem Versand von Trojanern erreichten die Strafverfolger "nur noch den DAU, aber doch nicht die Schwerstkriminellen und Terroristen, die sich hüten werden, auf Computern Spuren zu hinterlassen".

<http://www.heise.de/newsticker/meldung/85471>

[B]20.02.2007 11:39

Google protestiert gegen deutsche Pläne zur Vorratsdatenspeicherung [/B]

Der Referentenentwurf aus dem Bundesjustizministerium zur Neuregelung der Telekommunikationsüberwachung, mit dem auch die EU-Vorgaben zur Vorratsspeicherung von Telefon- und Internetdaten in deutsches Recht umgesetzt werden sollen, stößt international auf Widerstand. So hat sich nun der europäische Konzerndatenschutzbeauftragte von Google, Peter Fleischer, von Paris aus entschieden gegen das Gesetzesvorhaben ausgesprochen. Der Jurist stößt sich vor allem an einer Auflage, wonach auch Anbieter von E-Mail-Konten künftig Kundendaten erheben und Nutzer so eindeutig identifizieren sollen. "Das ist unglaublich schlecht für den Schutz der Privatsphäre", empörte sich Fleischer gegenüber der New York Times über den Vorstoß. Die Nutzer hätten sich insbesondere im Kampf gegen Spam an die Möglichkeit gewöhnt, eine anonyme E-Mail-Adresse zu haben.

Als besonders "ironisch" bezeichnete Fleischer angesichts der demnächst im Bundeskabinett zu besprechenden Pläne zugleich die Tatsache, dass "Deutschland eines der Länder in Europa ist, wo die Menschen am meisten über Datenschutz reden". Allgemein würde er das Land der Dichter und Denker aber beim tatsächlichen Schutz der Privatsphäre "an das hinterste Ende stellen". Zudem sei die Anforderung an die Anbieter "überhaupt nicht zu kontrollieren und würde niemals funktionieren." Es gehe viel zu weit, dass man voraussichtlich wohl gar einen Personalausweis für die Beantragung eines E-Mail-Postfachs vorlegen müsse. Zumal sich deutsche Surfer bei E-Mail-Providern etwa in den USA nach wie vor E-Mail-Adressen ohne Identitätsprüfung besorgen und weiterhin etwa Googles Gmail, Yahoos Webmail oder Microsofts Hotmail nutzen könnten.

Deutlich vorsichtiger nähert sich ein Sprecher der Branchenvereinigung Bitkom im Gespräch mit der US-Zeitung dem Umsetzungsvorhaben an: "Es gibt nicht viele Leute in Deutschland, die den Entwurf vollständig unterstützen", meint der Verbandsvertreter. "Aber es gibt andere, die ihm noch kritischer gegenüberstehen als wir." Ende Januar hatten 27 zivilgesellschaftliche Organisationen unter der Führung des Arbeitskreises Vorratsdatenspeicherung scharfen Protest gegen den Plan des Justizministeriums eingelegt, künftig "Daten über jede Nutzung von Telefon, Handy, E-Mail und Internet auf Vorrat" sammeln zu lassen. Es sei "inakzeptabel", dass ohne jeden Verdacht auf eine Straftat sensible Informationen über die sozialen Beziehungen, die Bewegungen und die individuelle Lebenssituation der über 80 Millionen Bundesbürger erfasst werden sollen. Damals hatte auch der Bitkom gegen "eine weitere Aushöhlung des grundrechtlich geschützten Fernmeldegeheimnisses" Stellung bezogen und wieder einmal auf die fehlende Regelung zur Kostenentschädigung der betroffenen Unternehmen für die Hilfssheriffsdienste hingewiesen.

Generell sollen Telekommunikationsanbieter mit dem Gesetzesentwurf verpflichtet werden, Verbindungs- und Standortdaten sechs Monate lang verdachtsunabhängig auf Vorrat vorzuhalten. Der Entwurf aus dem Justizministerium hält gemäß einem Beschluss des Bundestags daran fest, die Sicherheitsbehörden auch bei "mittels Telekommunikation begangener Straftaten" in den Datenbergen schürfen zu lassen. Die entsprechende EU-Richtlinie sieht einen Zugriff zunächst nur bei "schweren Straftaten" vor.

<http://www.heise.de/newsticker/meldung/85568>

Tetrarchos - 21.2.2007 um 01:47

Mit den üblichen Totschlagargumenten wird das am Ende wieder durchgesetzt: "Wir bekämpfen Terrorismus blabla..." Oder: "Wir bekämpfen Kinderporno im Internet blabla..."

Die Unverhältnismäßigkeit der Methode, wird dann wieder vom Volk geschluckt. Mißbrauch mit dem Mißbrauch, sozusagen!
Ob die Regierung wohl schon ein gefaktes Terrorattentat in Deutschland plant? Als Vorwand für totalen Polizeistaat??
Mir schiesst grade eine Ganze "neue" Idee durch den Kopf, warum grade JETZT die Monhaupt freikommt? Ob man der dann was anhängen will??

... - 22.2.2007 um 05:22

Nö, dafür haben die ja immer ein paar bekloppte Islamisten, die das auch machen, ohne dass der Staat da einschreitet. Und wenn, nur über V-Leute, die in den Gruppen sitzen, vom Verfassungsschutz.

Aber immerhin **6 Anschlagversuche seit 2000**.

Mann, da fühlt man sich ja fast so von bedroht, wie von Dampfwalzen, die einem eine wilde Verfolgungsjagd liefern, wenn man in einem Ferrari sitzt.

Xoc - 22.2.2007 um 16:10

Ich persönlich bin ja dafür das Internet zum völlig rechtsfreien Raum zu erklären.
Wem's nicht passt, der soll draussen bleiben.
Und der arme Kommerz, der dann keine Sicherheit mehr hat, dem weine ich nun eine Krokodilsträne hinterher.
Oder vielleicht ein alternatives Kommerznet zum Internet, in dem beliebig abgemahnt, überwacht und gegängelt werden darf.

Tetrarchos - 23.2.2007 um 03:10

Wenn mans geschickt anstellt, ist das internet ja nahezu rechtsfrei.Man muss aber regelrecht Arbeit darein stecken, um sowas zu machen.Proxyserver ist mal ein Anfang.Aber für das weitere muss man schon länger lernen.Wenn man wirklich gut sein will...

MAUS - 14.3.2007 um 14:28

[B]IT-Exportinitiative wirft Regierung "Überwachungsgier" vor[/B]

34 Firmen der deutschen IT-Sicherheitsbranche, die sich zu einer Exportinitiative zusammengeschlossen haben, lehnen Pläne des Bundesinnenministers für verdeckte Online-Durchsuchungen ab. Laut einer Mitteilung der Initiative "IT Security Made in Germany" (ITSMIG) sagte einer ihrer Sprecher, Frank Fuchs: "Schon allein die Diskussion, ob in Deutschland auf Computerfestplatten die Kernbereiche privater Lebensführung vom Staat durchschnüffelt werden dürfen, schadet uns nachhaltig im Ausland."

Der Bundesgerichtshof (BGH) untersagte jüngst das heimliche Ausspähen von Festplatten über das Internet wegen fehlender Rechtsgrundlage. Bundesinnenminister Schäuble und Polizeivertreter dringen seitdem auf eine gesetzliche Regelung, die den Strafverfolgern und den Geheimdiensten die staatliche Verwanzung von PCs erlaubt. Datenschützer und Bundesjustizministerin Brigitte Zypries (SPD) hegen dagegen weiterhin schwere rechtliche Bedenken gegen die geplante Schnüffeltechnik.

Bislang hätten die deutschen Anbieter im internationalen Wettbewerb Vorteile, meint die ITSMIG nun zu den Plänen für eine heimliche Online-Durchsuchung. So gelte die deutsche Herkunft Anwendern als Garant, vor undokumentierten Hintertüren verschont zu bleiben. Die ITSMIG verweist auf das Beispiel der USA, wo Politiker immer wieder unter Berufung auf den Kampf gegen Terrorismus forderten, staatlichen Stellen eine Überwachung durch die Hintertür zu ermöglichen. Den dortigen Anbietern falle es schwer, glaubwürdig zu versichern, dass bei ihren Produkten die US-Behörden nicht mithören.

Die ITSMIG wurde vom Bundeswirtschaftsministerium als unabhängige Plattform gegründet und vom Fraunhofer-Institut für Sichere Informationstechnologie SIT konzipiert und umgesetzt. Sie geht davon aus, dass bereits das Bekanntwerden der Pläne die deutsche IT-Sicherheitsbranche und die Herkunftsbezeichnung "Made in Germany" diskreditiere und deren Vertrauenswürdigkeit unterhöhle. "Dass der deutsche Staat uns in seiner Überwachungsgier nun einen 'Bundestrojaner' unterjubeln will, ist katastrophal", sagte ITSMIG-Mitglied Antonius Sommer. Er und Fuchs schlagen den Begriff "Bundestrojaner" als Unwort des Jahres 2007 vor. Die Initiative präsentiert sich auf der CeBIT in Halle 7, Stand D22/10.

1999 habe die Bundesregierung in ihren Eckpunkten zur Kryptopolitik verdeutlicht, dass sie in der Verwendung sicherer Verschlüsselung eine entscheidende Voraussetzung für den Datenschutz der Bürger und für den Schutz von Unternehmensgeheimnissen sieht. Außerdem wollte sie Maßnahmen ergreifen, um die internationale Wettbewerbsfähigkeit deutscher Hersteller von sicheren Verschlüsselungsprodukten zu stärken. Dem widersprächen nun die Pläne für Online-Durchsuchungen, erläutert die ITSMIG.

<http://www.heise.de/newsticker/meldung/86605>

14.03.2007 10:32

[B]Demo gegen den Überwachungswahn in Frankfurt [/B]

Nach Protestzügen in Berlin und in Bielefeld im vergangenen Jahr laden Bürgerrechtler nun für den 14. April zu einer bundesweiten Demonstration gegen die "ausufernde Überwachung durch Staat und Wirtschaft" nach Frankfurt am Main ein. Besorgte Bürger sollen wieder unter dem Motto "Freiheit statt Angst" auf die Straße gehen. Startpunkt ist um 15 Uhr am Hauptbahnhof. Den Abschluss des Protestmarsches durch die Innenstadt soll eine Kundgebung vor der traditionsreichen Paulskirche bilden, wo 1848 die ersten Grundrechte auf deutschem Boden erarbeitet wurden. Heute bedroht die "grenzenlose Sicherheitslogik der Politik" den Veranstaltern zufolge die historische Errungenschaft der Verfassung.

Der Überwachungswahn greife um sich, heißt es in dem Aufruf zum Demonstrieren. Mit der geplanten Vorratsspeicherung von Telefon- und Internetdaten sowie Online-Durchsuchungen von Computern stünden weiter verschärfte Sicherheits- und Überwachungsbefugnisse auf der politischen Agenda. Dabei bewirke die zunehmende elektronische Erfassung und Überwachung der gesamten Bevölkerung keinen verbesserten Schutz vor Kriminalität, sondern koste vielmehr Millionen von Euro und gefährde die Privatsphäre Unschuldiger. "Wo Angst und Aktionismus regieren, bleiben gezielte und nachhaltige Maßnahmen zur Stärkung der Sicherheit ebenso auf der Strecke wie ein Angehen der wirklichen, alltäglichen Probleme der Menschen", verweisen die Organisatoren auf einen halbherzigen Kampf etwa gegen Arbeitslosigkeit und Armut.

Zu den Initiatoren des dritten Protestzugs gegen die Überwachungsgesellschaft gehören der Arbeitskreis Vorratsdatenspeicherung sowie 11 weitere Organisationen vom Chaos Computer Club (CCC) über den FoeBuD und die Piratenpartei Hessen bis zu STOP1984. An den beiden bisherigen Veranstaltungen dieser Art hatten sich jeweils zwischen 250 und über 300 Demonstranten beteiligt.

Konkret fordern die Organisatoren neben einem Nein zur "Totalprotokollierung" der Telekommunikation und zu geheimen Computerdurchsuchungen ein Ende der Videoüberwachung des öffentlichen Raums, einen Verzicht auf eine

automatische Gesichtskontrolle sowie den Stopp von Biometrie und RFID-Chips in Ausweisen und Pässen. Ferner wenden sie sich erneut gegen eine Aufzeichnung des Flugreiseverkehrs und einen automatischen Kfz-Kennzeichenabgleich auf öffentlichen Straßen, wie ihn immer mehr Polizeigesetze der Länder erlauben. Die Veranstalter plädieren dafür, alle seit 1968 beschlossenen Überwachungsgesetze auf ihre Effektivität und schädlichen Nebenwirkungen hin unabhängig überprüfen zu lassen. Die Arbeiten an neuen Kontrollgesetze sollen sofort beendet werden. (Stefan Krempf) / (jk/c't)

<http://www.heise.de/newsticker/meldung/86698>

14.03.2007 11:22

[B]Abhörgesetz in Schweden vorerst gescheitert [/B]

Das geplante neue schwedische Abhörgesetz ist vorerst gescheitert. Das Gesetz wurde in der vergangenen Woche ins Parlament eingebracht und am Montag und Dienstag dort diskutiert. Das Abhörgesetz fand selbst bei den Parteien des konservativ-liberalen Regierungsbündnisses keine ausreichende Unterstützung, berichtet die Frankfurter Allgemeine Zeitung. Es sollte zum 1. Juli in Kraft treten und der zum Militär gehörenden Funkabhöranstalt (Försvarets Radioanstalt) das Recht erteilen, ohne konkreten Verdacht und ohne richterlichen Abhörbeschluss den grenzüberschreitenden elektronischen Verkehr (Telefongespräche, Faxe, E-Mail & SMS) abhören zu können. "Da ein großer Teil der elektronischen Kommunikation der Schweden über ausländische Server läuft, wäre dies einer nahezu vollkommenen Überwachung der Schweden gleichgekommen", heißt es in dem Bericht.

Ausschlaggebend für die Ablehnung des Abhörgesetzes waren offenbar mehrere Stellungnahmen von IT-Experten, laut denen es technisch nicht möglich sei, zwischen nationalen und internationalen Mails so zu unterscheiden, dass die Suchprogramme der Funkabhöranstalt die innerschwedische Kommunikation von der Überwachung ausnehmen können. Dementsprechend zeichnete sich in der Debatte im schwedischen Reichstag ab, dass neben den linken Oppositionsparteien auch der größte Teil der ebenfalls in der Opposition befindlichen Sozialdemokraten stimmen werden. Außerdem hatten Abgeordnete aus dem Regierungslager ihren Widerstand gegen das Gesetz angekündigt. Damit gilt das Abhörgesetz als gescheitert.

Das Gesetz selbst war die modifizierte Variante eines Abhörgesetzes, mit dem die damals regierenden Sozialdemokraten gescheitert waren und muss jetzt erneut überarbeitet werden. Bis auf weiteres darf die Funkabhöranstalt nur den Funkverkehr abhören. Sie wurde vor 50 Jahren gegründet, um den sowjetischen Funk belauschen zu können. (Detlef Borchers) / (anw/c't)

<http://www.heise.de/newsticker/meldung/86705>

MAUS - 15.3.2007 um 13:05

14.03.2007 13:22

[B]Beckstein fordert "höchste Wachsamkeit" besonders an Hochschulen [/B]

Der bayerische Innenminister Günther Beckstein hat sich heute hinter eine E-Mail gestellt, die die Verwaltung der Ludwig-Maximilian-Universität (LMU) gestern an alle Mitarbeiter verschickt hatte. Diese wurden nach dem Propaganda-Video vom Wochenende, das mit Terroranschlägen in Deutschland wegen des Afghanistan-Einsatzes drohte, zur "höchsten Wachsamkeit" aufgefordert. Unverzüglich sollen alle "verdächtig erscheinende Wahrnehmungen", die irgendwie auf eine "islamistisch-fundamentalistische Haltung" schließen lassen, gemeldet werden.

Der bayerische Innenminister Beckstein forderte heute die ganze Bevölkerung dazu auf, "höchste Wachsamkeit" zu leisten und "bei Auffälligkeiten" sofort die Sicherheitsbehörden zu informieren. "Die jüngsten Terrordrohungen gegen Deutschland sind ernst zu nehmen. Die Sicherheitsbehörden sind hoch sensibilisiert. Auch wenn derzeit keine Hinweise auf konkrete Anschlägeplanungen in Deutschland bestehen, ist größte Wachsamkeit gefordert, um mögliche Anschlägeplanungen so frühzeitig wie möglich aufdecken zu können. Dazu kann auch jeder Einzelne beitragen. Bei Auffälligkeiten sollten Sicherheitsbehörden unbedingt informiert werden." Besonders an den Universitäten sei hohe Aufmerksamkeit erforderlich. Man müsse auf "Studenten und Mitarbeiter" achten, "die sich durch besondere Verhaltensweisen wie einen Bruch im Lebenswandel, Gewaltbereitschaft, radikal-verbale Äußerungen oder Beschäftigung mit einschlägiger Literatur auffällig in Richtung islamistischer Fundamentalismus verändern."

Gestern hatte Beckstein bereits in einem Interview auf die erhöhte Gefahr von "so genannten Home Grown Terrorists,

das heißt in Deutschland geborenen potenziellen Tätern", hingewiesen. Erforderlich seien auch mehr "Cybercops" für Internetermittlungen. Und bei der Gelegenheit forderte er auch wieder die Möglichkeit von Online-Durchsuchungen: "Es muss auch die Möglichkeit zu Online-Durchsuchungen von Festplatten bestehen, wenn der Verdacht schwerster Straftaten vorliegt. Dafür muss die Bundesregierung eine Rechtsgrundlage schaffen. Die SPD sollte hier nicht länger blockieren."

<http://www.heise.de/newsticker/meldung/86722>

14.03.2007 - 16:43 Uhr

[B]FTD: Uni München bedauert Aufruf zur Islamisten-Suche [/B]

Die Ludwig-Maximilians-Universität München (LMU) hat einen Aufruf zur Meldung mutmaßlich islamistischer Studenten bedauert. Bei einer hochschulintern versendeten E-Mail handelt es sich angeblich um ein Missverständnis. Trotzdem könnten andere Unis folgen.

"Es war ein Fehler, aber Fehler passieren", sagte LMU-Rektor Bernd Huber am Mittwoch über die E-Mail. Darin wurden Mitarbeiter aufgefordert, wachsam zu sein und verdächtige Studenten und Kollegen unverzüglich zu melden.

Absender der Mail war ein Abteilungsleiter, den die Universitätsleitung vor Kurzem als Ansprechpartner für den bayerischen Verfassungsschutz ernannt hatte. Anlass für die Aufforderung war ein Video, das islamistische Fundamentalisten am Wochenende verbreitet hatten. Darin warnte ein verummter Sprecher Deutschland und Österreich vor Anschlägen, sollten sie sich nicht aus Afghanistan zurückziehen. Das Drohvideo löste in der bayerischen Staatsregierung große Befürchtungen aus. "Fanatisierte islamistische Gruppen in Deutschland könnten sich durch den Aufruf zu einem Anschlag verleiten lassen", sagte Innenminister Günther Beckstein am Dienstag der "Passauer Neuen Presse".

"Es geht um eine Sensibilisierung"

LMU-Rektor Huber betonte, seine Universität sei liberal und weltoffen. Man sei froh über alle Studenten aus dem Ausland. Der Professor bedauerte zudem, dass die E-Mail missverstanden worden sei. Er sei strikt gegen eine Atmosphäre der Bespitzelung. Die Formulierung der E-Mail sei zu weit gegangen. Der Rektor sagte jedoch auch, dass das Gefahrenpotenzial nicht kleingeredet werden dürfe: "Es geht um eine Sensibilisierung."

Der Kanzler der LMU, Thomas May, hatte am Dienstag bestätigt, dass die E-Mail am Montag auf Anregung des Landesamts für Verfassungsschutz verschickt wurde. Sie richtet sich an einen breiten Adressatenkreis in der Universitätsverwaltung. Mitarbeiter wurden darin zu "hoher Wachsamkeit" aufgefordert. Sie sollten auf Studenten und Mitarbeiter achten, "die sich durch besondere Verhaltensweisen, wie zum Beispiel einen Bruch im Lebenswandel, Gewaltbereitschaft, radikal-verbale Äußerungen oder Beschäftigung mit einschlägiger Literatur auffällig in Richtung islamischer Fundamentalismus verändern".

Die Vorsitzende der Grünen, Claudia Roth, hatte die E-Mail als "vollkommen überzogen" kritisiert. "Ein solcher Aufruf erzeugt ein Klima der Hexenjagd, das uns im Kampf gegen internationalen Terrorismus nicht weiterbringt", sagte sie der FTD.

Warnung vor Hexenjagd

Das bayerische Innenministerium hatte das Vorgehen am Dienstag als "Teil der Aufmerksamkeitsstrategie" verteidigt. "Wir haben an den Universitäten die Situation, dass wir Studenten aus Problemstaaten haben, die hier interessantes Know-how lernen können", sagte ein Sprecher des bayerischen Innenministeriums.

Andere Hochschulen könnten ähnliche Aufrufe verschicken. Nach Angaben von May hatte der Verfassungsschutz die Kanzler sämtlicher Universitäten Bayerns bereits vor vier Wochen aufgefordert, Ansprechpartner für eine Zusammenarbeit zu benennen.

Autor/Autoren: Nikolai Fichtner (Berlin)

<http://www.finanztreff.de/ftreff/news.htm?id=26963565&sektion=ftd&u=0&k=0>

... - 16.3.2007 um 02:54

Sehr gut.
Ich find' das gut, dass die sich auf studierende Moslems konzentrieren und nicht etwa auf in der Behindertenarbeit tätige Protestanten. :D

MAUS - 20.3.2007 um 12:52

Know-how

11.03.2007 07:02

[B]Jürgen Schmidt

Bundestrojaner: Geht was – was geht

Technische Optionen für die Online-Durchsuchung[/B]

Die meinen das Ernst: Das unbemerkte Durchsuchen von PCs durch Ermittlungsbehörden soll gesetzlich geregelt und anschließend auch technisch umgesetzt werden. Und rein technisch wäre das sogar machbar. Doch erst bei genauer Betrachtung zeigt sich, in welches Dilemma die Behörden dabei geraten.

Einige Spekulationen rund um das heimliche Ausforschen von Internet-PCs kann man schnell aussortieren. Selbst wenn es – wie im Kontext des sogenannten NSA-Keys vermutet – tatsächlich eine Hintertür in Windows geben sollte, käme die für solche Zwecke kaum zum Einsatz. Käme die Existenz einer solchen Hintertür raus – und das würde sie früher oder später – wäre es ein PR-GAU ohnegleichen. Und es ist kaum vorstellbar, dass ein multinationaler Konzern wie Microsoft das Wohl & Wehe seines Aktienkurses der Schweigsamkeit eines deutschen Polizisten anvertraut.

So ganz ohne weiteres kann man nicht von außen die Daten eines Rechners zugreifen; im Regelfall wird der Netzwerkverkehr des Zielsystems gefiltert. Auf Systemen mit direktem Internet-Zugang kommen oft Personal Firewalls zum Einsatz, in vielen Fällen erledigt diese Aufgabe aber auch ein externer Router mit Firewall-Funktionen, der nur ausgehenden Verkehr zulässt. Zugang für Online-Durchsuchungen über eine Hintertür in Firewalls ist zwar technisch möglich aber schon aufgrund der Vielfalt eher unwahrscheinlich. Somit muss man irgendwas an der Firewall vorbeischmuggeln, was dann die Tür von Innen öffnet.

[B]Aufgabenteilung[/B]

Dabei ist es sehr naheliegend, dass sich der Bundestrojaner an der Architektur moderner Schädlinge orientiert, die eine strikte Aufgabenteilung vornehmen: die Infiltration und die eigentliche Spionage. Bei der Infiltration geht es darum, einmalig die Sicherungsmechanismen des PCs zu umgehen und ein kleines Programm zur Ausführung zu bringen. Gefragt ist hier also ein typisches trojanisches Pferd.

Einmal im Innern lädt der Trojaner das eigentliche Überwachungsmodul nach, das sich dann im System einnistet, dort versteckt, Daten sammelt und diese entweder aktiv nach außen verschickt oder solange bereit hält, bis sie abgerufen werden. Das entspricht vom Anforderungsprofil einer Mischung aus Spyware und Rootkit. Der weitere Text unterscheidet folglich zwischen einer Trojaner- und einer Spyware-Komponente.

Diese Trennung in zwei Komponenten bringt eine Reihe von Vorteilen mit sich. Insbesondere kann man das trojanische Pferd vergleichsweise einfach und schnell neu erstellen, um Viren-Signaturen auszuweichen oder es sogar individuell auf die Zielperson maßzuschneidern. Die technisch anspruchsvollere Spyware-Komponente hingegen kommt erst zum Einsatz, wenn man bereits einen Treffer gelandet hat und wird somit keinem unnötigen (Entdeckungs-)Risiko ausgesetzt.

[B]Pferdezucht[/B]

Die Trojaner-Komponente wird eine Form von Downloader sein, der das Spyware-Modul von irgendwo aus dem Netz nachlädt und startet. Sowas ist schnell entwickelt und auf Grund der recht unspezifischen Beschreibung schwer zu identifizieren. Ausgehende Verbindungen lassen sich immer irgendwie als normaler Netzwerkverkehr tarnen und am Anwender und dessen Schutz-Software vorbeimogeln, wenn man es drauf anlegt.

Spannend ist die Frage, wie dieser Downloader auf das Zielsystem gelangt und dort aktiviert wird. Da gibt es im wesentlichen drei Szenarien. Das einfachste: Etwas wie die Rechnungs-Trojaner "in gut". Wenn die Profifahnder im Rahmen ihrer Ermittlungen ohnehin bereits Informationen über den Verdächtigen gesammelt haben, haben sie dafür beste Voraussetzungen. Sie könnten dem Verdächtigen unter der tatsächlichen Adresse eines Freundes mit passender persönlicher Ansprache ein "geiles Spiel" oder einen zum Hobby passenden Bildschirmschoner unterjubeln. Und wenn es nicht auf Anhieb funktioniert, ist es auch nicht weiter schlimm: Ein Virus mehr in der Inbox wird kaum Verdacht erregen.

[B]Zwangseinleitung[/B]

Eine andere Variante wäre das Einschleusen des Bundestrojaners in ohnehin durchgeführte Downloads. So wäre es durchaus möglich, Provider per Gesetz dazu zu verpflichten, spezielle Proxies aufzustellen. Auf eine entsprechende Anordnung wird der dann der Zielperson bei der nächsten Einwahl als transparenter Zwangs-Proxy zugeordnet, über den alle Verbindungen umgeleitet werden, sodass er den nächsten Download mit dem Bundestrojaner infizieren kann.

Das funktioniert wie bei klassischen Viren: Der Schadcode hängt sich hinten an die ausführbare Datei an, und ersetzt Code im Programm durch einen Sprung auf den eigenen. Die überschriebenen Befehle werden gespeichert und vor dem Rücksprung ausgeführt. Technisch gesehen ist das keine große Sache: Derartige Infektionstechniken sind gut untersucht und der Aufwand, einen existierenden Proxy entsprechend aufzubohren, sollte überschaubar sein.

Mit dem nächsten Spiel oder Utility, das die Zielperson aus dem Internet herunterlädt und startet, holt sie sich auch den Trojaner auf den Rechner. Das naheliegendste Ziel für einen solchen Angriff wären automatisch installierte Sicherheits-Updates, da diese oft sogar ohne Zutun des Anwenders installiert werden. Doch da hat Microsoft einen Riegel vorgeschoben: Die Sicherheits-Updates tragen eine digitale Signatur aus Redmond. Wenn deutsche Beamte am Update herumfummeln, zerstören sie diese Signatur und der Update-Service verweigert die Installation. Analog sichern beispielsweise auch Mac OS X, SuSE und Ubuntu ihre Sicherheits-Updates. Aber dann klinkt sich der Bundestrojaner eben in den Download der nächsten Firefox-Version ein.

Im Vergleich zu der Variante mit dem Trojaner per Mail oder Instant Messenger bedeutet dieses Verfahren zwar deutlich mehr Aufwand, dafür garantiert es zumindest auf den ersten Blick einen bürokratisierbaren und weitgehend reibungslosen Ablauf. Dass die Politiker durchaus bereit sind, auf Wunsch der Strafverfolger alle Provider dazu zu verpflichten, technische Gerätschaften nach ihren Vorgaben aufzustellen, haben sie mit der Telekommunikationsüberwachungsverordnung (TKÜV) demonstriert. Sie verpflichtet die Provider bereits seit 2005 eine "Standardschnittstelle zur Ausleitung von E-Mail an die Strafverfolgung" bereitzuhalten. Da passt eine "Standardschnittstelle zur Einleitung von Überwachungssoftware der Strafverfolgung" doch prima ins Regal daneben.

[B]Schwarzer Spion[/B]

Und schließlich bleibt immer noch die Variante, Sicherheitslücken in Applikationen auszunutzen, wie es bereits bei der Industriespionage geschieht. In Abständen von wenigen Wochen melden Antivirenhersteller beispielsweise immer wieder neue Office-Dateien, die bislang unbekannte Sicherheitslücken in Microsofts Office-Programmen ausnutzen, um Spionage-Software zu installieren. Und das sind nur die Fälle, in denen der virtuelle Einbruch aufgefliegen ist.

DOC-, MP3-, MOV-, PDF- aber auch JPG-Dateien könnten über Lücken in Abspiel- oder Anzeigeprogrammen zum Einfallstor werden. Mit etwas Vorbereitung kann man sowas jedem unterjubeln, der das Internet nutzt. Der Haken: Die zwei von Schäuble angeheuerten Entwickler werden solche Lücken kaum aufspüren. Und auf dem freien Schwarzmarkt sind diese sogenannten Zerodays recht teuer. Da legt man schnell mal 10.000 Euro für einen Exploit auf den Tisch, der nach dem ersten Einsatz unter Umständen schon verbrannt ist, weil er entdeckt wurde. Ganz abgesehen davon, dass der Einkauf in dieser Szene moralisch ziemlich fragwürdig wäre. Diese Version wird also vermutlich auch weiterhin Geheimdiensten und freiberuflichen "Informationsbeschaffern" vorbehalten bleiben, die jeden Preis zahlen.

[B]Der weisse Spion[/B]

Softwaretechnisch deutlich aufwendiger ist die Spyware-Komponente. Muss sie sich doch im System über Tage, Wochen oder sogar Monate verstecken, im Hintergrund Informationen sammeln und diese auf Abruf übers Netz an den Ermittler weiterleiten. Und das alles auch noch in beweiskräftiger Form. Doch darüber müssen sich Schäubles Beamte nicht weiter den Kopf zerbrechen. Das gibt es nämlich schon – und sogar zu kaufen.

Encase von Guidance Software ist die Software für professionelle Beweismittelsicherung schlechthin; unter anderem FBI und BKA setzen sie ein. Und deren Hersteller bietet mit dem sogenannten Field Intelligence Model (FIM) zufällig ein Produkt an, dessen Beschreibung durchaus der Nährboden für Schäubles Überwachungsideen sein könnte:

Ein unauffälliger, passiver Software Agent mit Auto-Update, der auf den zu überwachendenn Arbeitsplatzsystemen oder Servern installiert wird. [...] Die Servlets haben spezielle Stealth-Funktionen und laufen auf folgenden Betriebssystemen: Alle Windows Versionen, Linux Kernel 2.4 und aufwärts, Solaris 8/9 mit 32/64 Bit und Mac OS X.

Wie das konkret funktioniert, bleibt leider offen, denn wie nicht anders zu erwarten, reagierte Guidance auf die Anfragen von heise Security zu Encase FIM nicht. Da man laut Produktbeschreibung ohnehin "ausschließlich an Strafverfolgungsbehörden" liefert, kann man Öffentlichkeit in dem Geschäft nicht brauchen.

[B]Alles muss versteckt sein[/B]

Im Gegenteil: Gerade das Verstecken der Software dürfte eines der Hauptprobleme sein. Zwar konnte auf Nachfragen

keiner der zehn befragten AV-Hersteller Signaturen für das Encase FIM-Servlet vorweisen. Doch die ließen sich ohnehin durch Modifikationen am Quellcode leicht umgehen.

Der Beschreibung nach zu urteilen, müsste aber auch jedes Behaviour Blocking, das seinem Namen auch nur halbwegs gerecht wird, die Aktivitäten eines derartigen Spyware-Programms bemerken. Denn wenn der Antiviren-Software ein Programm wie FIM durch die Maschen geht, gelingt das Spionageprogrammen aus kriminellen Quellen auch.

Ob die Antiviren-Software den Fund dann aber auch meldet, steht auf einem anderen Blatt. Zumindest theoretisch wäre es durchaus denkbar, dass sie in solchen Fällen mal ein Auge zudrückt. Marktführer Symantec wollte jedenfalls schonmal Fragen zu Encase FIM nicht beantworten.

Konkurrent Microsoft hingegen bezog deutlich Stellung zugunsten seiner Kunden: "Unsere Software meldet jedes verdächtige Verhalten, das ihr auffällt." Allerdings sei man dabei natürlich immer an die Gesetze eines Landes gebunden, schränkte Pressesprecher Thomas Baumgärtner im Hinblick auf die aktuelle Diskussion ein. Auch Dirk Kollberg von McAfees Avertlabs verneinte die Existenz diesbezüglicher Absprachen mit staatlichen oder sonstigen Behörden.

Da es ziemlich unwahrscheinlich ist, dass sich alle Hersteller auf Mauscheleien mit deutschen Behörden einlassen, wäre gleich das nächste Gesetz fällig: ein gesetzlich verordneter blinder Fleck für Sicherheitssoftware, damit sie den Bundetrojaner gewähren lässt. Schließlich darf es nicht sein, dass ein Softwarehersteller Millioneninvestitionen des deutschen Staates einfach hinfällig macht, indem er die Verdächtigen vor der Installation des Spyware-Moduls warnt.

Andererseits werden beispielsweise amerikanische Kunden keine Antiviren-Software kaufen, die bekanntermaßen eine "deutsche Hintertür" enthält. Es wird also zumindest im Ausland weiterhin AV-Software ohne geben – und genau die werden Kriminelle natürlich bevorzugt einsetzen. Das bedeutet im Umkehrschluss dann, dass früher oder später Forderungen auftauchen, den Einsatz von Sicherheitsoftware ohne diesen blinden Fleck in Deutschland zu verbieten, nach dem Motto: Es kann doch nicht angehen, dass sich kriminelle Subjekte den vom Gesetz legitimierten Durchsuchungen durch Strafverfolgungsbehörden erfolgreich entziehen.

[B]Konflikte[/B]

Letztlich ergibt sich durch den Bundestrojaner für die Behörden ein unlösbarer Interessenkonflikt: Einerseits fordern und fördern sie Sicherheitsmaßnahmen – und auf der anderen sind es genau diese Sicherheitsmaßnahmen, die ihnen den Zugriff auf die gewünschten Information verwehren. Entweder verbietet man effiziente Schutz-Software oder man versucht genau diese Schutz-Software immer wieder auszutricksen – und findet sich dabei in der Gesellschaft von Kriminellen wieder.

Jedes Loch in Sicherheitssoftware kann auch für Betrugereien, Spionage oder andere kriminelle Aktivitäten genutzt werden – insbesondere, wenn der Bundestrojaner schon demonstriert, wie das geht. Und wenn Beamte Kenntnis von solchen Lücken hätten und nicht für ihre Beseitigung gesorgt haben, träfe sie zumindest eine Mitverantwortung.

Und um Missverständnissen vorzubeugen: Selbstverständlich kann man sich gegen all die hier geschilderten Einbruchsversuche schützen. Gegen Trojaner in der Mail hilft konsequentes Nachfragen beim angeblichen Absender vor dem Öffnen eines Dateianhangs. Eventuelle Manipulationen von Trojaner-Proxies werden durch digitale Signaturen, Vergleiche von Prüfsummen und SSL-Downloads entlarvt. Selbst das Encase FIM Servlet lässt sich ziemlich sicher mit speziellen Antirootkit-Tools und entsprechendem Knowhow aufspüren und neutralisieren. Und die potenziellen Zielpersonen staatlich angeordneter Überwachungsmaßnahmen werden mit bei den ersten sein, die diese Wissen konsequent nutzen, um sich zu schützen. (ju)

<http://www.heise.de/security/artikel/86415/0>

[B]18.03.2007 11:52

Bosbach fordert schnelle Legalisierung von Online-Durchsuchungen [/B]

In der Debatte um eine neue Rechtsgrundlage für die staatliche Online-Durchsuchung von Computern macht die Union weiter Druck "Wir können auf das wichtige und wirksame Ermittlungsinstrument nicht verzichten, weil das Internet auch viele Gefahren birgt", sagte der stellvertretende Unions-Fraktionsvorsitzende Wolfgang Bosbach in einem dpa-Gespräch.

Der CDU-Innenpolitiker verwies darauf, dass sich die Terrororganisationen weltweit der Kommunikation über das Internet zunehmend bedienen. Die kürzlich von islamistischen Extremisten verbreiteten Warnungen an Deutschland

seien nur ein Beispiel. Sie nutzten das Internet aber vor allem für die interne Kommunikation. "Die Online-Durchsuchung dient der Sicherung von flüchtigen Beweisen, die den Behörden ohne rechtzeitigen Zugriff dauerhaft verloren gehen würden", fügte er hinzu.

Bosbach räumte ein, dass es sich bei der Online-Durchsuchung um einen erheblichen Eingriff in die Privatsphäre des Betroffenen handele. Deshalb dürfe sie nur mit einem richterlichen Beschluss und bei einem erheblichen Tatverdacht vorgenommen werden. Es sei aber unverantwortlich, eine Regelung komplett zu unterlassen.

Zuvor hatte auch Bayerns Justizministerin Beate Merk (CSU) eine schnelle gesetzliche Regelung verlangt. Schleswig-Holsteins Justizminister Uwe Döring (SPD) hält die Online-Razzia für nach wie vor verfassungsrechtlich bedenklich und zweifelt am Nutzen dieser Fahndungsmethode.

Der Bundesgerichtshof hatte das heimliche Ausspähen über das Internet durch staatliche Ermittler wegen fehlender Rechtsgrundlage Anfang Februar verboten. Seither gibt es Diskussionen, ob eine rasche Gesetzesänderung angestrebt werden soll. Der Bundesrat hatte sich vor mehr als einer Woche gegen eine rasche gesetzliche Regelung ausgesprochen. (dpa) / (tig/c't)

<http://www.heise.de/newsticker/meldung/86959>

[B]Sicherheitssoftware soll keine Ausnahme für Polizei-Trojaner machen[/B]

FBI und BKA wollen bei der Terrorfahndung in private Rechner eindringen. Solche Online-Durchsuchungen stoßen bei der Sicherheitssoftware-Branche auf Ablehnung. Sie wollten in ihren Programmen keine "Hintertür" für Ermittlungsbehörden offenlassen, betonen führende Antiviren-Spezialisten auf der CeBIT. Zugleich aber räumen sie ein: Ein gut geplanter und gezielter Angriff kann die besten Schutzmauern durchbrechen.

Für Mikko Hyppönen vom finnischen Antivirensoftware-Hersteller F-Secure ist der Fall klar: "Wir dürfen nicht zwischen 'bösen' und 'guten' Trojanern unterscheiden. Wir haben für uns beschlossen, dass wir sie alle entdecken und stoppen wollen." Jede Ausnahme wäre ein gefährlicher Präzedenzfall, betont Hyppönen. "Man stelle sich nur vor, wenn alle möglichen Geheimdienste und Sicherheitsbehörden verschiedener Länder bei Sicherheits-Spezialisten vorstellig würden."

Technisch statt politisch sieht seine Aufgabe auch der russische Antiviren-Spezialist Eugene Kaspersky: "Sicherheitssoftware ist wie ein Metalldetektor am Flughafen. Wenn er eine Waffe erkennt, schlägt er Alarm, egal ob sie von Terroristen oder von der Polizei ist." Außerdem seien Sicherheitssoftware-Updates international identisch. "Das heißt also: Entweder wir schützen die ganze Welt und auch Deutschland vor einem Trojaner – oder setzen alle der Gefahr aus."

Microsoft als Hersteller von Windows und seit einiger Zeit auch von Antivirensoftware ist in einer schwierigeren Situation. "Die Loyalität zum Kunden hat 100-prozentige Priorität", betont Firmensprecher Thomas Baumgärtner. Nur eben, dass nicht nur die Computernutzer Microsoft-Kunden seien, sondern auch die Regierung. Microsoft werde sich nie "gegen das Gesetz verhalten". Allerdings sei das Ganze eine hypothetische Diskussion: "Noch hat uns niemand um irgendetwas gebeten."

Eine ganz andere Frage allerdings ist, in wie weit die Software- Hersteller das Eindringen eines so genannten "Bundestrojaners" etwa einer Ermittlungsbehörde überhaupt verhindern können. "Jeden Schutz kann man umgehen", heißt es von der Branche grundsätzlich. "Wenn die Jungs ihre Hausaufgaben gemacht haben, haben wir keine Chance", sagt Kaspersky. Solche gut vorbereiteten Angriffe seien aber Ausnahmefälle, bei denen gezielt bestimmte Computer ins Visier genommen würden – zum Beispiel bei Industriespionage.

Einblicke, was alles möglich ist, gab auf der CeBIT ein Verfassungsschutz-Mitarbeiter. So könne man zum Beispiel die Überwachungssoftware von einem präparierten USB-Speicherstick laufen lassen, während man vorgebe, nur ein Paar Fotos zeigen zu wollen. Mit Handy-Trojanern könne man das Mikrofon aktivieren und unbemerkt Gespräche mithören. Beim Verfassungsschutz dürften deshalb keine ungeprüften USB-Sticks an die Computer angeschlossen werden und Mobiltelefone müssten bei Besprechungen draußen bleiben.

Die Diskussion ist für die Branche nicht neu. Ende 2001 hatte ein Bericht für Aufsehen gesorgt, wonach das FBI an einem Trojaner arbeitete, der alle Tastaturanschläge aufzeichnet. Daraufhin wurde ein Mitarbeiter der Firma Symantec – Hersteller von Norton Antivirus – in einem Artikel mit der Aussage zitiert, man würde das FBI gewähren lassen, wenn

eine Anfrage käme. Über den Konkurrenten McAfee berichtete damals ein Journalist, das Unternehmen habe sogar selbst das FBI kontaktiert, um sicherzustellen, dass der Trojaner nicht versehentlich entdeckt werde. McAfee bestritt das vehement. Doch das Vertrauen in die Branche war zunächst beschädigt.

<http://www.heise.de/newsticker/meldung/86970>

Soulmirror - 20.3.2007 um 16:19

um mal was positives über diesen bundestrojaner zu sagen ☐

<http://www.gulli.com/news/w32-bka-trojan-bald-keine-2007-03-19/>

den trojaner können die sich eh sonstwohin stecken, jemand der halbwegs auf sicherheit achtet oder eben einen virenschanner up2date hält, der sollte mit dem viech net größere probleme bekommen.

Tetrarchos - 20.3.2007 um 18:04

Zitat

Original von Soulmirror

um mal was positives über diesen bundestrojaner zu sagen ☐

<http://www.gulli.com/news/w32-bka-trojan-bald-keine-2007-03-19/>

den trojaner können die sich eh sonstwohin stecken, jemand der halbwegs auf sicherheit achtet oder eben einen virenschanner up2date hält, der sollte mit dem viech net größere probleme bekommen.

Ich denke mal das ein Trojaner der Strafverfolgungsbehörden von keiner Firewall oder Sicherheitssoftware angesprochen wird. Die Regierung würde schon dafür sorgen, daß entsprechende Anbieter von Internetsicherheitsdiensten den Polizeitrojaner gezielt aus ihren Programmen aussparen, damit er immer funktioniert. Aktiv wehren kann sich dann nurnoch der Informatik-Profi, der sich selber ein Schutzprogramm erstellt. Außerdem können Spezialisten für die Polizei ständig neue Trojaner schreiben, so das der PC doch immerwieder infiziert werden kann. Oder es werden die Internetzugänge in Deutschland standardmäßig so abgeändert, daß man nurnoch ins Net kann wenn man ein mithören der Polizei im Vertrag akzeptiert. ☐

Hansi - 20.3.2007 um 18:15

quark. sicherheitssoftware wird ja nich nur in deutschland produziert, und bei den ausländischen software unternehmen hat die deutsche regierung schonma gar nix zu melden. desweiteren können von dir benannte private computerexperten ihre selbstgeschriebenen progs als freeware bereitstellen. somit bliebe dann wieder wettkampf zwischen programierern die die dinge loslassen und denen die sie stoppen. und ich glaube auch nicht, dass sich die i-net anbieter in ihre agb's reinlabern lassen.

MAUS - 28.3.2007 um 14:19

24.03.2007 01:06

[B]Innenministerium: Verfassungsschutz, MAD und BND können Online-Durchsuchungen durchführen [/B]

Erst vor wenigen Tagen hatte die Bundesregierung auf eine Anfrage der FDP-Fraktion erklärt, dass das Bundesamt für Verfassungsschutz schon jetzt das Recht besitze, Online-Durchungen durchzuführen, obgleich der Bundesgerichtshof am 31. Januar dies untersagt und die Schaffung einer rechtlichen Grundlage gefordert hatte. Nun hat die Bundesregierung auf eine Anfrage von Wolfgang Wieland, des innenpolitischen Sprechers der Grünen-Fraktion, mitgeteilt, dass nicht nur der Verfassungsschutz, sondern auch der Militärische Abwehrdienst (MAD) und der Bundesnachrichtendienst (BND) bereits die Rechtsgrundlagen „für eine heimliche Informationserhebung mittels Online-Durchsuchung“ besitzen. Im Inland würde der BND von seinen Befugnissen aber keinen Gebrauch machen. Die Anfrage hat der parlamentarischen Staatssekretär im Bundesinnenministerium, Peter Altmaier (CDU), beantwortet.

Ob die genannten Dienste bereits Online-Durchsuchungen durchführten, geht offenbar aus dem Schreiben nicht hervor. Wieland ist jedoch der Überzeugung: "Die Geheimdienste hacken bereits, ungeniert und unkontrolliert." Er fordert die

Bundesregierung auf, die Online-Durchsuchungen sofort einzustellen. Für Wieland wird damit Art. 13 GG (Unverletzlichkeit der Wohnung) verletzt, da es sich bei Online-Durchsuchungen auf Festplatten heimischer PCs um ein Eindringen in Wohnungen handelt. Überdies sei mit dem Eindringen in Computer auch nicht der vom Bundesverfassungsgericht geforderte Schutz des "Kernbereichs privater Lebensgestaltung" gewährleistet. Wieland moniert, dass die Online-Durchsuchungen, so sie denn bereits praktiziert werden, unkontrolliert stattfinden würden. Weder liege für sie eine Genehmigung eines Richters vor, noch werde sie von der G-10-Kommission kontrolliert. Das sei ein Skandal.

Gegenüber Spiegel Online wies ein Sprecher des Bundesinnenministeriums die Vorwürfe zurück und berief sich auf die Gesetzeslage: "Das Bundesverfassungsschutzgesetz ist für jedermann offen und lesbar. Was die konkrete Tätigkeit der Nachrichtendienste angeht, berichten wir aber nur an das Parlamentarische Kontrollgremium (PKG) und nicht an die Öffentlichkeit. Auch das ist kein Skandal, sondern der Wille des Gesetzgebers." Dem Handelsblatt erklärte eine Sprecherin des Bundesamts für Verfassungsschutz auf die Frage, ob bereits Online-Durchsuchungen stattgefunden hätten, dass dies geheim sei. Zudem unterliege auch die Dienstvorschrift, aufgrund derer dies geregelt ist, der Geheimhaltung. Nach Paragraph 8 Absatz 2 des Bundesverfassungsschutzgesetzes dürfen die Verfassungsschützer nach der zur Geheimsache erklärten Dienstvorschrift "Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung anwenden". Auch Dieter Wiefelspütz, innenpolitischer Sprecher der SPD-Bundestagsfraktion, hatte am Dienstag bereits erklärt, die Bundesregierung sei der Meinung, für Online-Durchsuchungen bereits eine Rechtsgrundlage zu haben, betonte aber, eine "klare Rechtsgrundlage" müsse man erst schaffen. So äußerte sich auch Wolfgang Bosbach, der stellvertretende Vorsitzende der CDU/CSU-Fraktion, während Jörg Ziercke, der Präsident des Bundeskriminalamtes, forderte, dass der Gesetzgeber dieses Fahndungsmittel ermöglichen müsse.

Wieland wirft der Bundesregierung vor, sie wisse sehr wohl, dass die von ihr beanspruchte Rechtsgrundlage nicht gesicherte ist. Nach dem Schreiben werde nämlich aufgrund des Beschlusses des Bundesgerichtshofs geprüft, ob "gegebenenfalls ein gesetzgeberischer Änderungsbedarf bei der entsprechenden Informationsbeschaffung durch die Nachrichtendienste besteht". (fr/Telepolis)

<http://www.heise.de/newsticker/meldung/87316>

[B]Die Mutter aller Terror-Datenbanken quillt über[/B]
Florian Rötzer 26.03.2007

[B]Nach drei Jahren hat sich Terrorist Identities Datamart Environment (TIDE) des National Counterterrorism Center mindestens vervierfacht[/B]

In den USA wurden nach dem 11.9. neben dem neuen Ministerium für Innere Sicherheit, dem Department for Homeland Security, zahlreiche Antiterror-Einheiten mitsamt Terrorlisten geschaffen. Im Kern steht das National Counterterrorism Center (NCTC), bei dem alle Informationen über Terrorismus aus dem Inland und dem Ausland zusammenlaufen sollen und das entsprechend Zugriff auf viele Datenbanken besitzt. Das NCTC betreut auch die zentrale Datenbank Terrorist Identities Datamart Environment (TIDE), in der seit 2003 alle geheimen Informationen von allen Quellen wie der CIA, der DIA, dem FBI oder der NSA gesammelt und analysiert werden. Aus der TIDE-Datenbank gehen Informationen etwa zum Terrorist Screening Center (TSC) des FBI, das die unterschiedlichen Beobachtungslisten (watch lists) zusammenstellt, beispielsweise die No-Fly-Liste für die Transportbehörde TSA, die Visa- und Passliste für das Außenministerium oder die Liste für das National Crime and Information Center (NCIC) des FBI.

Das NCTC betreut auch die "geheimste Website der Welt", so sieht es jedenfalls John Scott Redd, der ehemalige Vizeadmiral und jetzige Direktor des NCTC. Auf der Website, kurz NOL genannt, werden Geheimdienstinformationen von 28 Regierungsnetzwerken bzw. 60 Behörden aufbereitet, so dass ein schneller Zugriff weltweit von Mitarbeitern der Geheimdienste und Sicherheitsbehörden über die Informationen möglich ist, die über Terroristen und Verdächtige vorliegen. 2006 waren hier nach einem NCTC-Bericht bereits 6 Millionen Dokumente zugänglich, die wiederum mit TIDE abgeglichen werden.

Das Problem ist, wie es bei allen Terrorlisten zu erwarten ist, die alles scheinbar Verdächtige sammeln, dass mit dem steigenden Informationsberg auch die Unübersichtlichkeit wächst und die Qualität der Informationen abnimmt. Gesammelt werden vom NCTC nicht nur "Terroristen" im Ausland und verdächtige Ausländer, sondern erstmals auch verdächtige US-Bürger in einer Datenbank. Mittlerweile enthält TIDE Informationen zu 435.000 Namen (mit Aliasnamen) von Terroristen oder Terrorverdächtigen bzw. Dateien von über 300.000 Einzelpersonen.

Russ Travers, der verantwortlich für TIDE ist, zeigt sich gegenüber der Washington Post bereits besorgt über die

"langfristige Qualitätskontrolle". Allerdings müsste er nicht in die Zukunft schauen, es gab bereits zahlreiche Fälle, bei denen Menschen aufgrund einer Namensverwechslung oder falschen Informationen in die Maschinerie des Terrorverdachts kamen. 2004 und 2005 lag nach einem Bericht des Government Accountability Office bei der Hälfte der Namen von Reisenden, bei denen eine Überprüfung aufgrund der Liste zum NSC erbeten wurde, ein Irrtum vor. Das betraf auch US-Politiker wie den demokratischen Senator Ted Kennedy oder die Frau des republikanischen Senators Ted Stevens, dessen Frau Catherine Stevens mehrmals bei Flügen einen Warnhinweis ausgelöst hatte, weil man sie offenbar mit Cat Stevens verwechselte. Der ist zwar Muslim geworden, aber auch hier wäre schon die Frage, was er auf der Liste der Verdächtigen zu suchen hat.

Aufgrund der Geheimhaltung und der unregulierten Kompetenz des NCTC ist es kaum möglich, wieder von den Listen gestrichen zu werden, was Travers gegenüber der Washington Post auch einräumt. Offenbar kommt sicherheitshalber vieles in die Datenbank, was nicht wirklich überprüft wurde. Und ganz nach Behördenmaxime behält man lieber alles, weil man ja nie wissen kann. Das ist hier ohne weiteres möglich, weil die Datenbank eine black box ist und niemand das Recht hat, auch wenn er fälschlicherweise hineingeraten ist, die Behörde zu zwingen, die Daten nachweisbar zu löschen.

Tausende von Informationen kommen täglich zu TIDE, berichtet Travers. Vieles sei fragmentarisch, inkonsistent und falsch. Man nehme auf, was als vernünftig verdächtig gelten könne. Verdächtige erhalten Nummern, denen alles zugeordnet wird, was über die Person gesammelt wurde und bekannt ist. Sunnitische und schiitische Muslime stellen die Mehrzahl, angeblich sind nur 5 Prozent US-Bürger dabei, die aufgenommen werden, wenn es irgendeine Verbindung zum internationalen Terrorismus gebe.

Jeden Tag werden die neuen Informationen und Personen in die Datenbank des TSC eingespeist. Dort sind mittlerweile Informationen über 235.000 Menschen gespeichert, nachdem die von Tide kommenden Daten noch einmal überprüft wurden. Angeblich würden nach einer weiteren Überprüfung die Zahl derjenigen, die schließlich auf der No-fly-Liste der TSA, die 30.000 Namen enthalten soll – nach Informationen von CBS sollen es aber schon letztes Jahr 44.000 gewesen sein -, oder den Listen für die Konsulate, der Grenzbehörden oder der Polizei landen, noch geringer sein. Die Liste der Verdächtigen, die genauer überprüft werden müssen, bevor sie in die USA einreisen können, ist allerdings wesentlich größer als die auf der No-fly-Liste. Auch hier bleibt geheim, nach welchen Kriterien selektiert wird.

Sogar 14 der 19 Flugzeugentführer vom 11.9. waren zumindest noch letztes Jahr auf der Liste. Das verteidigte Rick Kopel, der Direktor des NSC noch heute. Terroristen würden nämlich gerne Namen benutzen, von denen sie glauben, sie stünden nicht auf den Terrorlisten: "Bei jedem Namen auf der Liste gibt es einen Grund, warum er sich dort befindet."

<http://www.heise.de/tp/r4/artikel/24/24939/1.html>

27.03.2007 09:04

[B]BKA-Präsident: Online-Durchsuchung klappt ohne Schadsoftware [/B]

Bei einem Fachgespräch der Grünen im Bundestag am Montag zum Thema "Bürgerrechtsschutz im digitalen Zeitalter" warb der Präsident des Bundeskriminalamts (BKA), Jörg Ziercke, weiter für verdeckte Ermittlungen im Internetbereich. Zuvor hatte er in einem taz-Interview erklärt, solche Durchsuchungen seien "hochprofessionell" und keinesfalls eine "Schleppnetzfangdudung".

Es handle sich bei den geplanten Programmen zu den umstrittenen Online-Durchsuchungen nicht um "Schadsoftware", erklärte Ziercke während des Fachgesprächs der Grünen. Eingesetzt würden "keine Bundestrojaner", also keine Applikationen, durch die sich Daten löschen oder verändern lassen würden. Das Gerede von einer vom BKA verbreiteten Malware mit Schadroutinen sei "Kinderkram", wettete Ziercke, denn "so funktioniert kriminalistische Arbeit nicht". Hintertüren würden nicht offen gelassen. Vertreter des Chaos Computer Clubs (CCC) und Forscher warnten dagegen vor einem Kontrollverlust der Nutzer und der bewussten staatlichen Schaffung von Sicherheitslücken.

Ziercke brachte mehrere "Sicherungsmaßnahmen" ins Spiel, um Kollateralschäden bei der Online-Durchsuchung von Festplatten und virtuellen Speichern zu verhindern. So habe die zumindest theoretisch inzwischen klarer umrissene Software eine "Steuerungskomponente", um sie nach der von einem Richter freigegebenen Einsatzzeit wieder abzuschalten. Es würden natürlich auch "nur bestimmte, identifizierte Dateien übertragen", nicht der komplette Inhalt von 300-Gigabyte-Festplatten. Eine Erkennung der Schnüffelkomponente durch Anti-Virensoftware werde durch die Verbreitung in Einzelfällen verhindert. Am Anfang stehe eine "eindeutige Identifikation des Zielsystems". Eine Unterstützung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Programmierung des heimlichen Ermittlungswerkzeugs ist laut dem BKA-Chef nicht erforderlich. Der BSI-Präsident Udo Helmbrecht hatte

zuvor versprochen, das Bestmögliche für die IT-Sicherheit in Deutschland zu tun: "Wir sind die Behörde, der Sie vertrauen sollten."

"Wir müssen keine Schwachstellen ausnutzen", orakelte Ziercke weiter. Der Quellcode "einer solchen Untersuchung" könne zudem beim Gericht hinterlegt werden, machte er einen weiteren Vorschlag zur rechtsstaatlichen Fassung der geforderten Maßnahme. Dies setze voraus, "dass sich die Justiz in diesem Bereich fachlich fortentwickelt." Aber auch Experten etwa vom CCC will er im Nachhinein Zugang zu der Programmblaupause einer eingesetzten Applikation gewähren. Zugleich nannte Ziercke eine Reihe konkreter Fälle, in denen er eine Online-Durchsuchung für unbedingt erforderlich hält. Dabei geht es etwa um den Austausch von Informationen zu Sprengvorrichtungen, eine konkrete Anschlagplanung, die Unterstützung für den internationalen Dschihad und die Anwerbung für ein Selbstmordattentat über das Internet, Recherchen zu einem möglichen Landesverrat durch die Weitergabe von Konstruktionszeichnungen und das Aufklären von Umtrieben eines fremden Geheimdienstes. Ziercke nannte als Anlass für eine Online-Durchsuchung auch die Unterstützung für ein Terrornetz, bei denen der Verdächtige Internet-Telefonie sowie E-Mail-Verschlüsselung nutze beziehungsweise im "Entwurfsmodus" online kommuniziere, also die E-Mail jeweils nur im Entwurfsordner im Web abgelegt und gar nicht versandt werde.

Einen Phishing-Fall zählte der oberste Kriminalbeamte der Republik ebenfalls mit auf, in dem der Versand der trügerischen Mails über ein Bot-Netz mit zehntausenden Rechnern weltweit erfolgt sei. In den genannten Beispielen ist laut Ziercke ein heimliches Vorgehen essenziell, um tatsächlich an die Täter-Netzwerke zu gelangen und diese nicht etwa durch eine offene Hausdurchsuchung bereits frühzeitig zu warnen. Zuvor hatte er sich wiederholt über den Anstieg von Straftaten im Bereich Kinderpornographie sehr besorgt gezeigt.

Der Hacker starbug vom CCC führte dagegen vor, wie einfach ein Rechner mit Betriebssystem Windows XP durch die Ausnutzung einer bekannten Windows-Schwachstelle gleichsam ferngesteuert werden kann. Es sei mit einem Trojaner möglich, sich nicht nur etwa Fotos auf dem so geknackten PC anzuschauen oder gespeicherte E-Mails zu lesen. Man könne auch "Dateien raufschieben", einer Person also beispielsweise kinderpornographisches Material oder Bombenbauanleitungen unterjubeln. "Die ultimative Spionage-Software gibt es nicht", ergänzte die CCC-Abgesandte Constanze Kurz. Es müsse klar sein, "dass jede Schadsoftware ihrerseits Schwachstellen hat, zum Beispiel Programmierfehler". Diese könnten Kriminelle ausnutzen. Die zweite Gefahr sei, dass der "Bundestrojaner einfach entdeckt werden könnte, wenn er nach Hause telefoniert". In Folge würden sich "Wettbewerbe von Hackern" bilden, welche die Programme analysieren. Die Online-Durchsuchung sei zudem im größeren Zusammenhang all der anderen Überwachungsmaßnahmen wie der geplanten Vorratsspeicherung von Telefon- und Internetdaten zu sehen, die seit dem 11. September 2001 in der Gesamtschau den Bürger unter Generalverdacht stellen würden.

Andreas Pfitzmann, Informatikprofessor an der TU Dresden, bezeichnete es zudem als "extrem risikoreich", gute (Überwachungs-)Software für eine nicht genau bekannte Rechnerumgebung zu schreiben. Er wäre "extremst verwundert", wenn die Kenntnisse beim BKA in diesem Bereich die in der Forschung deutlich übersteigen würden und nicht doch ein "universelles trojanisches Pferd" herauskäme. Der Streit um den Bundestrojaner ist für Pfitzmann aber eine "Nulldiskussion", solange die gängige Computerinfrastruktur absolut unsicher sei. Er verglich die Rechnerlandschaft mit "Häusern, die so unsicher sind, dass Sie keinen Schimmer haben, ob da jetzt einmal, zweimal oder fünfmal Besuch da war." Man merke auch nicht, ob etwas weg oder dazu kam. In diesem Rahmen habe er weniger Angst vor dem deutschen Polizisten oder Geheimdienstler: "Aber Kriminelle werden die Möglichkeiten kumulativ nutzen."

Allgemein erinnerte Alexander Rossnagel vom Forschungszentrum für Informationstechnik-Gestaltung an der Universität Kassel an die Vorgaben des Bundesverfassungsgerichts, wonach auch Online-Durchsuchungen nicht zu einer Rundumüberwachung oder zu Eingriffen in den Kernbereich der privaten Lebensgestaltung führen dürften. Der Erlanger Strafrechtler Hans Kudlich tat sich schwer mit der Einordnung der Netzbespitzelung in die Grundrechte und die Strafprozessordnung. Er geht davon aus, dass Online-Durchsuchungen mit einer Verfassungsänderung ähnlich wie beim großen Lauschangriff verbunden sein müsste.

<http://www.heise.de/newsticker/meldung/87421>

27.03.2007 12:15

[B]Stärkung des "präventiven Datenschutzes" gefordert [B]

Angesichts der zunehmenden präventiven staatlichen Überwachung hat sich der Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), Thilo Weichert, als Korrekturmaßnahme für eine stärkere vorsorgliche Sicherung der Privatsphäre ausgesprochen. Ganz in diesem Sinne steht der am heutigen Dienstag veröffentlichte Tätigkeitsbericht 2007 des ULD (PDF-Datei) unter dem optimistischen Titel: "Der präventive Datenschutz

startet durch". Mit Leben gefüllt haben die Kieler Datenschützer diesen Begriff gemäß dem 180 Seiten umfassenden Report insbesondere mit den Instrumenten des Datenschutz-Gütesiegels und des vorgeschalteten Auditverfahrens. Hier haben die Schleswig-Holsteiner Weichert zufolge mit der umstrittenen Zertifizierung eines Updateproduktes von Microsoft "eine wichtige Schallmauer" durchbrochen und dem Prüfverfahren eine internationale Dimension verliehen.

Bei der EU-Kommission stehe zudem das Projekt EuroPriSe (European Privacy Seal) kurz vor der Genehmigung, das unter Leitung des ULD gemeinsam mit 6 weiteren europäischen Partnern das Gütesiegel des Landes europaweit verbreiten soll, freut sich der Chef der Einrichtung. Um auch den "bundesweit starken Zuspruch" zu befriedigen, verfolge man das Ziel einer bundesgesetzlichen Verankerung des Verfahrens. Gütesiegel und Audit seien aber nur zwei von einer Vielzahl weiterer Instrumente, mit denen der präventive Datenschutz vorangebracht werde. So gewinne die strukturelle Unternehmens- und Behördenberatung beim ULD eine immer wichtigere Bedeutung. Über den Vorsitz in der Arbeitsgruppe Versicherungswirtschaft der Datenschutzaufsichtsbehörden versucht die Einrichtung dabei, zunächst in einer Branche bundesweit Standards zu etablieren. Für ein gutes Datenschutzmanagement spreche, dass damit auch eine Optimierung des IT-Einsatzes und der Arbeitsabläufe erreicht werde.

Eitel Sonnenschein herrscht bei den Kieler Datenschützern aber nicht. "Im vergangenen Jahr kam es so zu einigen, teilweise auch öffentlich ausgetragenen Konflikten", konstatiert Weichert. So sei dem schleswig-holsteinischen Innenministerium etwa partout nicht klarzumachen gewesen, dass die Pläne für eine Polizeirechtsnovelle nicht nur verfassungsrechtlich höchst problematisch, sondern zugleich ein Bärendienst für die Polizei und die Sicherheit des Landes seien. "Einige gravierende Schutzlücken konnten im inzwischen verabschiedeten Polizeirecht geschlossen werden, doch blieben und bleiben einige mehr als fragwürdige Regelungen erhalten", moniert der ULD-Leiter. Seine Einrichtung werde nun etwa die Einführung des Kfz-Kennzeichen-Scannings, der Schleierfahndung sowie der elektronischen polizeilichen Vorgangsdokumentation kritisch begleiten. Darüber hinaus habe sich auch das Bildungsministerium bis zuletzt geweigert, bei seinen Planungen zu einer Schüler-Individualstatistik die Anforderungen des Datenschutzes zu berücksichtigen.

Ein Blick über die Elbe offenbart für Weichert zudem, "dass außerhalb unseres Landes der Datenschutz noch nicht ausreichend in unsere informationsgesellschaftliche Kultur Eingang gefunden hat". Mit dem Argument der Missbrauchs- und Kriminalitätsbekämpfung würden immer wieder neue Datenerhebungs- und Verarbeitungsbefugnisse gewährt und neue Verarbeitungssysteme in Betrieb genommen, wobei als "Sesam-öffne-Dich für Informationsbegehrlichkeiten" seit dem 11. September 2001 die Bekämpfung von Terrorismus und darüber hinaus immer wieder auch der Kinderpornographie diene. Mit der 2006 beschlossenen Anti-Terror-Datei etwa schreite für Weichert "die Vergeheimdienstlichung unseres Sicherheitsapparates weiter voran. Würde die vom Bundesinnenministerium geforderte geheime Online-Durchsuchung gesetzlich erlaubt, wäre dies ihm zufolge "bundesweit ein schwerer Schlag gegen die Informationssicherheit und das Vertrauen der Nutzer in die Integrität ihrer IT-Systeme".

"Systemsprenkende Wirkung" würde dem Bericht nach die Umsetzung der EU-Pläne einer mindestens sechsmonatigen Vorratsspeicherung von Verbindungs- und Standortdaten aus dem Telekommunikationsbereich haben. "Es ist trotz Einbeziehung von Millionen von Kreditkartendaten bei aktuellen Ermittlungen und der Rasterung von sämtlichen internationalen Banktransaktionsdaten bei SWIFT für US-Geheimdienste immer noch nicht in das Bewusstsein der Öffentlichkeit gedrungen, dass die elektronischen Spuren, die wir bei allen möglichen Gelegenheiten hinterlassen, zu einer beklemmenden Beschneidung unserer Grundrechte führen kann", beklagt Weichert eine fehlende Sensibilisierung der Bürger und der Politik. Nur so sei es zu erklären, "dass wir den millionenfachen Datenschutzverstoß durch SWIFT immer noch nicht beendet haben, dass das Bundeswirtschaftsministerium weiterhin munter seine Idee eines riesigen Bundes-Einkommensregisters mit dem freundlichen Namen Elena verfolgt oder dass von der Bundespolitik krampfhaft die Umsetzung der Vorratsdatenspeicherungs-Richtlinie weiterverfolgt wird."

Die Bürger müssen sich dem ULD-Chef zufolge stärker "über die Konsequenzen ihres informationstechnischen Tuns klar werden." Dies gelte für eine "unreflektierte Selbst- und Fremdentblößung im Internet unter dem neudeutschen Stichwort Web 2.0" wie für die "bedenkenlose Inanspruchnahme immer mächtigerer Internet-Angebote von Online-Monopolisten wie zum Beispiel Google". Der präventive Datenschutz bedürfe noch der weiteren Unterstützung der Wirtschaft, der Verwaltung, der Politik und generell der Öffentlichkeit. (Stefan Krempf) / (jk/c't)

<http://www.heise.de/newsticker/meldung/87441>

Kebap - 28.3.2007 um 14:32

CCCeBit 2007: Verantwortung für den Bundestrojaner abgelehnt

20. März 2007 (presse@ccc.de)

Hannover (20.03.2007) - Beim diesjährigen Versuch des Chaos Computer Club (CCC), dem Landesamt für Verfassungsschutz Nordrhein-Westfalen ein symbolisches Trojanisches Pferd zu überreichen, stießen die verblüfften Chaoten auf einen leeren Stand.

Das zuvor über den Besuch informierte Standpersonal des Verfassungsschutzes hatte offenbar mitsamt allen Plakaten und Broschüren die Flucht ergriffen. Zurück blieb nur ein ausgeschalteter Fernseher. Das mitgebrachte schwarz-rot-goldene Pferd konnte an niemanden mehr überreicht werden, verblieb daher symbolisch auf dem vorher penibel geräumten Tisch. "Augenscheinlich hat der Verfassungsschutz sein undemokratisches Wesen offenbart, indem er sich der Diskussion einfach entzogen hat," sagte CCC-Sprecher Andy Müller-Maguhn.

Hintergrund der Aktion ist die Diskussion um den sogenannten Bundestrojaner als Umschreibung für die verdeckte Online-Durchsuchung auf Privatrechnern. Das Landesamt für Verfassungsschutz Nordrhein- Westfalen hatte sich hier nicht nur mit einer konkreten technischen Lösung bekannt gemacht, das Bundesland NRW ist auch bislang das einzige, dass bereits eine rechtliche Grundlage für den Einsatz eines solchen Trojaners für die Geheimdienste geschaffen hatte.

Der CCC wendet sich ganz grundsätzlich gegen den Einsatz solcher Spionageprogramme gegen die Bürger. Der Bundestrojaner ist durch das heimliche und dauerhafte Ausspionieren zum Symbol für den Kontroll- und Überwachungsstaat geworden. Dass der Verfassungsschutz nicht einmal bereit war, den Negativpreis des CCC entgegen zu nehmen, zeigt deutlich, dass der Verfassungsschutz und das Innenministerium keine Bereitschaft an den Tag legen, den umstrittenen Einsatz des Bundestrojaners öffentlich zu diskutieren.

Bei einer normalen Hausdurchsuchung steht dem Betroffenen sowohl rechtlicher Beistand als auch eine Bezeugung und Protokollierung der durchgeführten Amtshandlungen zu. Dagegen bleibt die verdeckte Online Durchsuchung von Privat-Rechnern für den Ausspionierten unbemerkt.

"Das klammheimliche Manipulieren und Ausspähen von Privatrechnern durch Behörden ist nach unserer Ansicht für eine demokratische Gesellschaft höchst fragwürdig. Auch wenn Behörden nachvollziehbare Anliegen im Sinne der Staatssicherheit haben, müssen die Methoden überprüfbar bleiben. Bei einem verdeckten Trojaner kann sich der Betroffene nicht mehr gegen vermeintliche Beweise wehren, wenn der Rechner sich nicht mehr unter seiner Kontrolle befindet," fasste Club-Sprecher Andy Müller-Maguhn die Stellungnahme des CCC zusammen.

<http://www.ccc.de/press/releases/2007/20070320/>

... - 29.3.2007 um 02:38

Na, da wird der Verfassungsschutz aber enttäuscht sein, dass wir nur im öffentlichen Teil des Forums hier und da mal Überlegungen zu Anschlägen anstellen. :D

Aber das Ganze bringt mich auf eine Idee:

Als ich mit meinem damaligen Freund so in der 11./12. Klasse war, haben wir beide an den Bundesinnenminister geschrieben und darum gebeten, dass der Verfassungsschutz doch einfach mal unsere Verfassungstreue überprüfen sollte. Wir wären sehr geneigt, die Daten, die über uns gespeichert wären, zu erfahren und noch stärker, unsere Verfassungstreue mal so richtig unter Beweis zu stellen.

Mir hat dann irgendein Staatssekretär irgendwelche Infos über den Verfassungsschutz zugesandt, um mein "offensichtlich völlig realitätsfernes Bild über die Bundesrepublik und ihre Verfassungsorgane richtig zu stellen". Mein Freund hatte das noch anders formuliert und noch ein paar Mal den angeschrieben, um sich mit dem zu zoffen. Irgendwann schrieb dann der Staatssekretär, dass er einen Gedankenaustausch nicht mehr für sinnvoll hielt, da mein Freund die freiheitlich-demokratische Grundordnung, von dem der Staatstyp dauernd faselte, als "leere Phrase" bezeichnete.

Sollten wir nicht auch mal den Verfassungsschutz bitten, uns genauer zu untersuchen.

Wir würden offenbar das Bild von einer Sekte nicht los, in der sich auch neoliberale Kapitalismusfreunde und Nazis wohl fühlen könnten.

Und das muss doch nicht sein.:20:

ABER VORSICHT:

Kann schlimme Konsequenzen haben.

Mein damaliger Freund und ich sind beide heute im öffentlichen Dienst, er ist sogar Beamter geworden.:31:

Kebap - 2.4.2007 um 13:50

Seit dem 19. März 2007 wird die aktuelle ELSTER-Software für das Jahr 2006/2007 in der Version 8.1.0.0 [1] für den Steuerbürger bereitgestellt. Schon von Anfang an hegten Experten Zweifel an der Integrität der 18 MB großen .exe-Datei. Nach einer mehrtägigen intensiven Analyse fand der Chaos Computer Club (CCC) nun deutliche Hinweise, dass über die fragwürdige Software der sog. Bundestrojaner [2] verbreitet wird.

(Quelle: <http://www.ccc.de/updates/2007/bundestrojaner-elster>)

Der Bundestrojaner, kürzlich als neues Werkzeug des Überwachungsstaates in die Schlagzeilen geraten, soll das Ausspähen der gesamten steuerpflichtigen Bevölkerung ermöglichen. Jeder Bürger mit eigenem Einkommen wird in Zukunft verpflichtet, die Steuererklärung mittels ELSTER-Software abzugeben. Dass es dem CCC nach wenigen Tagen gelang, den Trojaner ausfindig zu machen, spricht nicht eben für die Qualität der Spitzelsoftware.

Die Analyse zeigte verschiedene verdächtige Module, wie z. B. wte0104-brsjm.digit, das u. a. vorhandene Mikrofone und Kameras in modernen Computern einschalten kann. Weitere Routinen dienen der Durchsuchung der auf dem Rechner gespeicherten Dateien. Eine Funktion sendet Daten vom Benutzerrechner ferngesteuert an den BKA-Rechner mit der IP-Adresse 217.7.176.25 [3].

Der Trojaner tauscht offenbar auch einige Systemdateien aus, um sich unabhängig vom ELSTER-Programm auf dem System einzunisten. Die Schadsoftware erzwingt danach einen Neustart des Rechners. Auf dem Bildschirm des betroffenen Computers erscheint dazu die Fehlermeldung: "Systemfehler 70797976 - Neustart erforderlich."

Pikanterweise wird ein Port auf dem infizierten Rechner geöffnet, der es erlaubt, neue Suchbegriffe nachzuladen. Das ist insofern problematisch, da die Suchfunktion eine Schwachstelle enthält, die es einem Angreifer erlaubt, nicht nur Suchbegriffe, sondern beliebige Daten und ausführbaren Code auf dem Rechner zu platzieren. "Damit ist der unbemerkten Manipulation aller Daten Tür und Tor geöffnet." sagte CCC-Spezialexperte Jens-Thorben Janckiewozki.

Eine erste Ausnutzung dieser Nachladeschwachstelle wurde auch schon in der freien Wildbahn beobachtet. Ein schwer zu analysierender, auf Schwachstellen des Bundestrojaners aufsetzender Wurm dient wahrscheinlich dem Abfangen von PIN- und TAN-Eingaben von Onlinebanking-Benutzern der Postbank. Auch erste Zusammenschlüsse von gekaperten Rechnern zu sogenannten Botnetzen wurden im Verlaufe des Samstags beobachtet. Der Chef des BSI hatte unlängst Botnetze als größte Gefahr im Internet ausgemacht.

Bisher war weder das BKA noch das Bundesinnenministerium für eine Stellungnahme zu erreichen. Unter der Hand gab ein Techniker des BKA jedoch zu, dass in den eigenen Reihen niemand den Trojaner programmiert hätte. Dafür mussten schon aus Kostengründen im Ausland Fachkräfte angeworben werden. Die großen Antivirenhersteller haben mittlerweile ebenfalls mit der Analyse begonnen und hoffen in den nächsten Tagen entsprechende Updates zu verbreiten.

* [1] <https://www.elster.de/>

* [2] <http://de.wikipedia.org/wiki/Bundestrojaner>

* [3] <http://www.ripe.net/whois?searchtext=217.7.176.25>

Darkeastwood - 2.4.2007 um 15:22

Zur Bekämpfung von Killerspielen, Kinderpornografie und extremistischen Gedankenguts ist dem Regime jedes Mittel recht. Nun sorgt ein neues Überwachungsinstrument für Aufsehen, welches direkt auf den Computer des Betroffenen eingeschleust werden soll. Wie soll das funktionieren?

Der Bundestrojaner ist ein Programm, welches über das Internet auf einen Rechner installiert wird und anschließend ständig im Hintergrund läuft. Dieses Programm kann dann beispielsweise alle Dateien nach Stichwörtern durchsuchen, überprüfen ob installierte Programme legal erworben wurden, die Aktivitäten des infizierten Rechners im Internet überwachen oder gleich Beweismaterial zum Staatsanwalt senden. Theoretisch gibt es kaum etwas, was sich durch den Einsatz dieses Trojaners nicht anstellen lässt.

Die entsprechende Verfassungsschutznovelle solle noch 2007 bundesweit in Kraft treten und damit die rechtlichen Grundlagen für eine Onlineüberwachung ebnen. Damit wird in Zukunft die Produktion, der Vertrieb und der Besitz verbotener Dateien wie Kinderpornografie, urheberrechtlich geschütztes Material oder extremistischen Äußerungen verboten. Um ein Entfernen des Bundestrojaner zu verhindern, wurde ein Abkommen mit allen deutschen Internet-Service-Providern geschlossen, dass von der Überwachung betroffene Personen, die ohne Bundestrojaner in das Internet wollen, vom entsprechenden Provider gesperrt werden. So wird es in Zukunft für mutmaßliche Raubkopierer, Kinderschänder und Extremisten nur noch Internet in Kombination mit den Bundestrojaner geben.

Der niedersächsische Innenminister Schünemann erklärt, dass mittels des Bundestrojaners die Präsenz von extremistischen Gedankenguts im Internet endlich beendet werden kann. So soll laut Vorstellungen der Innenminister, alle Treffpunkte von Extremisten im Internet gesperrt werden und Foreneinträge mit extremistischen Inhalten automatisch gelöscht werden.

Extremistische Seiten im Ausland sollen durch die deutschen Provider gesperrt werden. Ebenso will man mit Internetseiten, die raubkopierte Inhalte oder Kinderpornografie anbieten verfahren.

Ein weiterer Hauptschwerpunkt des Bundestrojaners liegt im Aufspüren von installierten Raubkopien, die sofort vom entsprechenden Computer entfernt werden können. Dabei wird vorher eine entsprechende Signatur der installierten Raubkopie an die Staatsanwaltschaft übertragen und vollelektronisch ein Strafverfahren eingeleitet. "Somit lassen sich die Fluten von Strafanzeigen im Bereich Urheberrechtsverletzungen erst bewältigen" erklärt Schünemann. Des Weiteren können P2P-Programme aufgespürt und beendet werden. "Durch den Bundestrojaner wird das Internet endlich wieder sicher", so Schünemann.

Tetrarchos - 2.4.2007 um 16:32

Da scheint den oberen 10.000 ja ganz gewaltig der Arsch zu gehen, vor einer Revolution die vom Internet den Start nehmen könnte?

Und natürlich wird das ganze fürs Dummvolk mit dem Totschlagargument "Kinderporno" legitimiert. Dabei gibt es bereits heute ausreichende Möglichkeiten um Besitzer von Kinderporno aufzuspüren.

Kebap - 2.4.2007 um 19:14

Bundesdatenschutz kritisiert Pläne für schärfere Sicherheitsgesetze

Der Bundesdatenschutzbeauftragte Peter Schaar hat die Vorschläge von Bundesinnenminister Wolfgang Schäuble (CDU) für eine rasche Verschärfung zahlreicher Sicherheitsgesetze kritisiert. Größere Befugnisse des Bundeskriminalamtes (BKA) bei der Verbrechensvorbeugung sehe er "ziemlich kritisch", sagte Schaar im WDR. "Denn gerade in diesem Vorfeld weiß man ja erst mal noch nicht so genau, wonach man sucht und nach wem man sucht." Er sei gespannt, "wie eine solche Regelung aussehen soll, die ganz gezielt terroristische Straftäter treffen soll und nicht etwa den normalen Bürger oder jemanden, der im Internet surft".

Schaar kündigte an, alle Vorschläge unter die Lupe zu nehmen. "Ich werde mir das sehr genau anschauen", sagte er. Die Maßnahmen müssten verhältnismäßig sein und dürften nicht zu tief in Bürgerrechte eingreifen. Trotz Terrorgefahr dürfe es nicht dazu kommen, "dass praktisch die Privatsphäre aller Bürgerinnen und Bürger wegen einer solchen Gefährdung letztlich nur in Gefahr gerät, sondern aufgehoben wird".

Schäubles Pläne zu erweiterten Ermittlungsbefugnisse für die Strafverfolger waren am Wochenende in Auszügen bekannt geworden. Nach den Vorstellungen des Bundesinnenministers sollen dem BKA künftig die heimlichen Online-Durchsuchungen von Computern erlaubt werden sowie die Rasterfahndung, also das Durchkämmen von Datenbanken auf der Grundlage vorher festgelegter Täterprofile. Zudem sollen die Daten aus der Lkw-Maut zur Aufklärung schwerer Verbrechen benutzt werden können. Quelle: <http://www.heise.de/newsticker/meldung/87745>

Übrigens, *diese* Datenbanksammlung, wird mal in die "Terrordatei" zusammengeführt:
<http://www.heise.de/ct/hintergrund/meldung/85995>

Nur mal ein paar Beispiele:
(Die Liste ist dreimal so lang)

AFIS-P - Personenidentifizierung
APR - Straftaten nach BtmG
TSC - Datei zur Bekämpfung synthetischer Drogen
FDR - Falldatei Rauschgift
DNA-Datei - Vorsorge DNA-Datei für künftige Verhütung von Straftaten
TaFaS - Taschendiebstahlsfahndungssystem
FUSION - Bekämpfung der Rockerkriminalität
GEW LINKS - Gewalttäterdatei Phänomenbereich „links“
GEW SPORT - Gewalttäterdatei Phänomenbereich Sport
EAO - Video Bahn Einrichtungsanordnung zur automatisierten offenen Videoüberwachung von Bahnanlagen
CARGO-INFO - Analysesystem Luftfracht, Express, Kurier- und Luftpostverkehr
Geschw. - Verdacht der landesverräterischen/geheimdienstlichen Agententätigkeit
Geschw. - Computersabotage und Datenveränderung
COLUMBUS - Informationsdatei Verbrauchssteuerhinterziehung
DAREX - Druckerzeugnisse, CD, DVD etc. politisch motivierte Kriminalität
FIU - Sammlung und Auswertung von Verdachtsanzeigen
G8 - Sammlung von Informationen zum G8-Gipfel in Heiligendamm
IgaSt - International agierende gewaltbereite Störer Globalisierungsgegner

Ja, da ist für jeden was dabei.

Tetrarchos - 4.4.2007 um 21:48

Geplant ist vor allem und am dringendensten eine ADRegK (= Allgemeine Datei Regierungs Kritiker). :12: Schliesslich braucht man ja Infos darüber WELCHE Personen gezielt mit Strafverfolgung und Verdächtigung abgeschossen werden sollen. :12:

MAUS - 7.4.2007 um 13:18

04.04.2007 11:29

[B]USA reklamieren "absolutes Recht" auf persönliche Daten von Europäern bei der Einreise [/B]

Vor seiner Reise nach Großbritannien hat der Chef des US-amerikanischen Department of Homeland Security Michael Chertoff in einem Interview mit dem britischen Telegraph noch einmal betont, dass die USA ein Recht darauf haben, alle von ihnen gewünschten persönlichen Daten von Europäern, die in die USA einreisen wollen, zu erhalten. Bis zum Juli soll ein neues Abkommen zur Übermittlung von Flugpassagierdaten (PNR) an die US-Sicherheitsbehörden ausgehandelt werden.

Datenschützer und Politiker fordern, die Weitergabe der Daten zu beschränken, die Verbindung mit weiteren Daten zu verhindern und die Speicherung zu begrenzen. Gewünscht wird überdies die Umstellung auf ein Push-Verfahren, bei dem die Fluggesellschaften die Daten an die US-Behörden übermitteln, die US-Regierung wünscht das Pull-Verfahren beizubehalten und will die PNR-Daten – bislang umfassen diese 34 Informationen von Namen über Geburtsdaten bis hin zu Kreditkartennummern, E-Mail-Adressen und Telefonnummern – mit weiteren Daten verbinden. So wurden die PNR-Daten bereits in das Computer Assisted Passenger Prescreening System II (CAPPS II) und dann in das Automated Targeting System (ATS) einbezogen, mit dem das Gefährdungspotenzial von Flugpassagieren ermittelt werden soll. Dort werden sie mit zahlreichen anderen Daten aus unterschiedlichen Datenbanken verknüpft. Die Daten werden bis zu 40 Jahre lang gespeichert. Sie stehen nicht nur anderen Behörden des Heimatschutzministeriums, sondern auch auf Anfrage dem FBI und anderen Sicherheitsbehörden offen.

Den Besuch bei seinem britischen Kollegen John Reid nutzt Chertoff aus, um wieder einmal Druck auf die EU auszuüben, auch wenn diese sich bislang für den Datenschutz nicht sonderlich stark macht. Seit 2004 war bekannt, dass die PNR-Daten für andere Überwachungsprogramme verwendet wurden. Chertoff erklärte, es bestünde die Sorge, dass künftige Terroranschläge von britischen oder europäischen Muslimen begangen werden könnten, die sich als "Bürger zweiter Klasse" empfinden und durch die "koloniale Vergangenheit" entfremdet fühlen. Im Gegensatz dazu würden die amerikanischen Muslime besser in die Gesellschaft integriert sein, da "das ganze Land ein Einwanderungsland ist" und deswegen die Unterscheidung zwischen Einheimischen und Außenseitern keinen Sinn mache.

Die USA würden zum Schutz vor Terroristen aus Europa mehrschichtige Sicherheitsvorkehrungen aufbauen und sich nicht darauf verlassen, "dass eine ausländische Regierung weiß, dass einer ihrer Bürger verdächtig ist und hierher reisen wird". Die Gefahr bestehe, dass ein "unbekannter Terrorist" dank des Visa-Waiver-Programms in die USA gelangen könne. Während man mit bekannten Verdächtigen keine großen Probleme habe, würden "Clean skin"-Verdächtige, deren "Dokumente völlig legitim und nicht gefälscht sind", eine Gefahr darstellen.

Um die erforderliche Sicherheit zu erlangen, müssten die USA von europäischen Reisenden zusätzliche Informationen wie E-Mail-Adressen oder Kreditkartendaten erhalten. Man werde nicht mit den Europäern darüber verhandeln, wer in die USA einreisen kann: "Wir haben ein absolutes Recht, die Informationen zu erhalten, ebenso wie ich das Recht habe, wenn jemand als Gast zu mir nach Hause kommen will, diesen zu fragen, wer er ist, und ihn sich ausweisen zu lassen." So sollen Reisende bald nicht mehr nur zwei Fingerabdrücke, sondern alle zehn abgeben müssen, wenn sie in die USA einreisen wollen, um so unbekannte Terroristen identifizieren zu können. Die USA bauen eine Datenbank auf, in der weltweit Fingerabdrücke gesammelt werden, die man an verdächtigen Orten gefunden hat.

Der Irak-Krieg habe die Welt nicht unsicherer gemacht, erklärte Chertoff in Übereinstimmung mit der Haltung im Weißen Haus. Zudem seien die USA jetzt sicherer und besser geschützt als vor dem 11. September 2001. Allerdings gebe es, besonders bei den Medien und in der "intellektuellen Klasse", die Neigung, nachzugeben. Das sei ein "sehr schädlicher und destruktiver Impuls". Schon letztes Jahr hatte Chertoff im Hinblick auf den Datenschutz vor einer zunehmend "aktivistischen, linken und elitären Rechtsphilosophie" gewarnt, die sich in Europa ausbreite. (fr/Telepolis)

<http://www.heise.de/newsticker/meldung/87842>

05.04.2007 08:11

[B]Kritik von Datenschützern ist für Bundesinnenminister Schäuble "naiv" [/B]

Bundesinnenminister Schäuble, gegenwärtig Ratsvorsitzender der EU-Innenminister, hat sich gestern zu einem Gespräch mit dem Berater des Präsidenten der Russischen Föderation Victor Ivanow, dem russischen Innenminister Raschid Nurgalijew, dem US-Minister für Homeland Security Michael Chertoff, dem stellvertretenden US-Justizminister Kenneth L. Wainstein und dem Vizepräsidenten der EU-Kommission und EU-Justizkommissar Franco Frattini getroffen. Dabei ging es um "Terrorismusbekämpfung, Grenzschutz und den Kampf gegen die Drogenproblematik in Afghanistan".

Schäuble nutzte die Gelegenheit, um für seine geplanten Sicherheitsmaßnahmen auf die "zunehmende Verflechtung von innerer und äußerer Sicherheit" durch den Terrorismus hinzuweisen. Bedroht seien die USA, Russland und die EU gleichermaßen von der "terroristischen Gefährdung", die sich "am Ausmaß der Gewaltbereitschaft, der logistischen Vernetzung und der langfristig angelegten und grenzüberschreitenden Vorgehensweise der Täter" zeige. Dass Russland mit dem Tschetschenienkonflikt oder die USA und einige EU-Mitgliedsländer mit dem Irak-Krieg eigene Probleme geschaffen haben, blieb dabei außen vor.

Die Gesprächspartner gaben mehr oder weniger verblümt ihre Positionen wieder. US-Heimatschutzminister Chertoff betonte den "internationalen Informationsaustausch", der zur Bekämpfung des Terrorismus notwendig sei und plädierte damit für weitgehende Abschaffung des Datenschutzes, die er auch an anderem Ort im Hinblick auf die Übermittlung der Flugpassagierdaten (PNR) forderte. Franco Frattini lobte überschwänglich, wie sich heute "Innen- und Außenpolitik gegenseitig befruchten". Victor Ivanow forderte eine bessere "strafrechtliche Verfolgung von Terroristen und ihren Unterstützern".

Einig war man sich, die Grenzkontrollen zu verschärfen und dabei auch mehr Informationen auszutauschen. Ganz allgemein seien sich, so die Mitteilung der Bundesregierung, die Teilnehmer einig gewesen, "dass die Bekämpfung des Terrorismus eines umfassenden Ansatzes und enger Kooperation bedarf. Hierbei kommt es auf die Durchführung von Ermittlungen, die Aufrechterhaltung wirkungsvoller Grenzschutzmaßnahmen, die Bekämpfung illegaler Reisetätigkeiten,

den Schutz kritischer Infrastrukturen und die Verhinderung von Radikalisierungstendenzen und Rekrutierungsbemühungen an".

Bundesinnenminister Schäuble machte in einem Interview mit dem Handelsblatt deutlich, was er unter dem Schutz des Terrorismus versteht. So könne man "zur Abwehr schwerer Gefahren ... unter Umständen stärkere Eingriffe vornehmen". Dazu gehöre auch, Computer heimlich durchsuchen zu können. Dafür müsse jetzt eine Rechtsgrundlage geschaffen werden, "damit zumindest für die Gefahrenabwehr das Instrument zur Verfügung steht. Terroristen kommunizieren nicht über Brieftauben". Es dürfe nicht sein, dass Verbrecher "besser ausgestattet sind als die Sicherheitsbehörden". Dazu sei es notwendig, auf den Datenfluss zwischen Computern und auf die Daten eines einzelnen Computers zugreifen zu können und, wenn nötig, das Grundgesetz zu verändern.

Die Kritik von Datenschützern ist für Schäuble "naiv" und irrelevant, die Menschen sieht der Innenminister hinter sich: "Es ist doch meine Aufgabe, für die Sicherheit der Menschen zu sorgen. Die große Mehrheit der Bevölkerung sieht das übrigens auch so." So verteidigt Schäuble auch, warum für ihn die Fingerabdrücke auch bei den Passämtern gespeichert werden sollen. Datenschützer sehen hier den Beginn einer zentralen Datenbank. Kritiker möchte Schäuble in die Schranken weisen: "Das Unbehagen an der Moderne kann aber nicht ausschließlich zu Lasten der inneren Sicherheit gehen. Wir dürfen nicht maßlos agieren, aber uns auch nicht wehrlos oder blind machen."

<http://www.heise.de/newsticker/meldung/87894>

05.04.2007 12:52

[B]Justizministerin lehnt Schäubles Vorschläge für Sicherheitsgesetze ab [/B]

Bundesjustizministerin Brigitte Zypries weist die Vorschläge des Kabinettskollegen Wolfgang Schäuble für neue Sicherheitsgesetze zurück. In einer Vorabmeldung des Nachrichtensmagazins Der Spiegel sagt sie, vieles, was derzeit diskutiert werde, sei in der Koalition nicht abgesprochen. Die bereits verabschiedeten Maßnahmen seien ihres Erachtens geeignet, die Gefahr von Terroranschlägen zu reduzieren. Zudem falle die akustische Wohnraumüberwachung zur Strafverfolgung in ihre Zuständigkeit und nicht in die des Bundesinnenministeriums, legt Zypries nach.

Zypries sieht keinen Grund, die bestehenden Möglichkeiten zur Wohnraumüberwachung zu erweitern. Die Nutzung von gespeicherten Fingerabdrücken aller Bundesbürger zur Gefahrenabwehr wäre aus ihrer Sicht "verfassungsrechtlich höchst bedenklich". Am vergangenen Wochenende war bekannt geworden, dass Schäuble eine Verschärfung von Sicherheitsgesetzen plant. Dazu gehören Präventivbefugnisse für das Bundeskriminalamt (BKA), Vereinfachungen beim großen Lauschangriff, Rasterfahndungen, heimliche Online-Durchsuchungen von Computern und die Nutzung der LKW-Maut-Daten zur Aufklärung schwerer Straftaten.

Der ehemalige NRW-Innenminister und Ex-Bundestagsvizepräsident Burkhard Hirsch geht in einem Gastbeitrag für die Süddeutsche Zeitung noch weiter als Zypries. Er sieht in der von Schäuble geplanten "Sicherheitsarchitektur" die Verwandlung der Bundesrepublik in einen Überwachungsstaat. "Die Zeit freundlicher Kritik und ständiger Mahnung, bei der Terrorismusbekämpfung Augenmaß zu wahren, geht zu Ende. Nun ist Widerstand geboten", schreibt Hirsch.

In seinem Artikel schildert er die Chronologie der gesetzlichen Maßnahmen, die infolge der Attentate vom 11. September 2001 ergriffen wurden, wie beispielsweise das vom Bundestag "im Blindflug" verabschiedeten "Otto-Paket". Abschließend bezieht er sich auf einen Aufruf der Humanistischen Union von 1978: "Man bekämpft die Feinde des Rechtsstaats nicht mit dessen Abbau, und man verteidigt die Freiheit nicht mit deren Einschränkung."

<http://www.heise.de/newsticker/meldung/87916>

MAUS - 12.4.2007 um 09:26

[B]Minister Schünemann (CDU) - erstaunlich und typisch [/B]

Berlin (NRhZ/DL, 8.4.) Uwe Schünemann, Innenminister von Niedersachsen (CDU): „Die Gefahr eines terroristischen Anschlags in Deutschland war noch nie so groß wie in diesen Tagen". Diese verschärfte Bedrohung, so Schünemann, ergäbe sich aus dem "Einsatz von Tornado-Kampfflugzeugen in Afghanistan". Dazu Petra Pau, stellvertretende Vorsitzende der Fraktion DIE LINKE und Mitglied im Innenausschuss: "Ich merke erstens an: Schünemann spricht von "Kampfflugzeugen" und nicht von Aufklärungs-Tornados. Diese Sprachklarheit ist für einen CDU-Politiker erstaunlich. Ich

merke zweitens an: Schünemann schlussfolgert, dass diese erhöhte Terrorgefahr zwangsläufig die "Durchsuchung privater Computer" und die "vorbeugende Telefon-Überwachung" erheische. Diese Logik ist für einen CDU-Innenminister typisch. Ich merke drittens an: Selten wurde die Gefahr deutlicher beschrieben, die der vermeintlichen Sicherheits-Politik der Union entspringt. Man schafft auswärts neue Gefahren, um inwärts Bürgerrechte zu schleifen."

http://www.nrhz.de/flyer/suche.php?ressort_id_menu=-1&ressort_menu=News

Kebap - 13.4.2007 um 15:39

<http://www.ueberwachungsdruck.org/>

Wiki mit vielen gesammelten Überwachungsinfos

MAUS - 17.4.2007 um 11:32

14.04.2007 16:05

[B]Zypries lehnt Fingerabdruck-Register für alle Passbesitzer ab[/B]

In den Kreis der Kritiker Wolfgang Schäubles (CDU) hat sich jetzt auch Bundesjustizministerin Brigitte Zypries (SPD) eingereiht. Den Vorschlag des Bundesinnenministers, neben den digitalen Fotos auch die Fingerabdrücke aller deutschen Reisepass-Besitzer in einem Register für die Polizei elektronisch verfügbar zu machen und dieses zur Fahndung einzusetzen, lehnt die SPD-Politikerin ab: "Der Staat würde die Daten dann für diese Bürger ein Leben lang speichern, um gegebenenfalls gegen einige, wenige vorgehen zu können. Gerade der Fingerabdruck aber ist eine höchst sensible Information – man hinterlässt ihn überall", sagte die Ministerin gegenüber Bild am Sonntag.

Im Zusammenhang mit den Vorschlägen Schäubles zur Verschärfung der Sicherheitsgesetze hat Zypries die Bundesregierung aufgefordert, die Sorgen der Bürger vor zu viel Überwachung ernst zu nehmen: "Wenn nun neue Vorschläge gemacht werden, dann müssen wir bei jeder einzelnen Maßnahme prüfen, ob sie sinnvoll und verfassungsgemäß ist", sagte Zypries. Es dürfe jedoch nicht nur die einzelne Maßnahme betrachtet werden, auch die Summe der staatlichen Eingriffe müsse geprüft werden. Wie die Online-Ausgabe der Tagesschau berichtet, steht Zypries auch den von Schäuble geplanten Zugriffen auf die bei den Meldeämtern gespeicherten digitale Passbilder durch die Polizei skeptisch gegenüber.

Wolfgang Schäuble hält mittlerweile seinen Kritikern in einem Interview mit der Welt Online vor, "nicht viele Kenntnisse über die Verfassung" zu zeigen: "Manche sagen bei allem, was ihnen nicht gefällt, es sei verfassungswidrig." Nach Sicht des Bundesinnenministers besteht kein grundsätzlicher Unterschied zwischen der bisherigen Praxis, die bei den örtlichen Behörden in den Akten vorliegenden Passfotos zu Fahndungszwecken an die Ermittler per Fax zu übermitteln und einer zukünftig möglichen Online-Übertragung: "Die Aufregung der SPD verstehe ich wirklich nicht." (pek/c't)

<http://www.heise.de/newsticker/meldung/88251>

14.04.2007 22:24

[B]Über 1000 Demonstranten protestierten gegen den Überwachungsstaat [/B]

In Frankfurt am Main setzten am Samstagnachmittag bei einer Demo nach Angaben der Veranstalter 1500 bis 2000 Bürgerrechtler ein Zeichen gegen eine "ausufernde Überwachung". Die Polizei schätzte die Zahl der Demonstranten auf etwa 1000. Unter dem Motto "Freiheit statt Angst" zogen die Demonstranten durch die Frankfurter Innenstadt und skandierten Sprechchöre wie "Stoppt den Überwachungswahn". Auf Plakaten verglichen sie die Privatsphäre mit Sauerstoff und wehrten sich dagegen, Datenschutz als "Verbrechen" abzustempeln.

Ganz aktuell wendete sich der Protest etwa gegen den heftig umstrittenen Plan von Bundesinnenminister Wolfgang Schäuble (CDU), im Rahmen eines neuen Anti-Terrorpakets das Überwachungsnetz deutlich auszubauen und etwa der Polizei einen automatischen Zugriff auf digitale Passbilder und später Fingerabdrücke aus Ausweisdokumenten zu ermöglichen. Weiter sprachen sich die Teilnehmer etwa gegen die im Raum stehende Vorratsspeicherung von Telefon- und Internetdaten, verdeckte Online-Durchsuchungen, die zunehmende Videoüberwachung öffentlicher Plätze, die Aufzeichnung des Flugreiseverkehrs und einen automatischen Kfz-Kennzeichenabgleich auf öffentlichen Straßen aus.

Zu der Kundgebung hatten unter der Führung des Arbeitskreises Vorratsdatenspeicherung mehr als 20 Organisationen

und Gruppen aufgerufen, darunter der Chaos Computer Club (CCC), die Grüne Jugend und der Bundesvorstand der Grünen, die Jungen Liberalen, Die Linke sowie Hochschul- und Menschenrechtsvereinigungen. Die Demonstration hatte deutlich mehr Zulauf als die beiden ersten Veranstaltungen dieser Art, an denen sich in Berlin und in Bielefeld im vergangenen Jahr jeweils zwischen 250 und 300 Personen beteiligten. Die momentan geführte hitzige Diskussion über weitere tief greifende Änderungen an der Sicherheitsarchitektur durch die von Schäuble angestrebte Stärkung der präventiven Überwachung dürfte ihren Teil zu dem wachsenden Zuspruch an derartigen öffentlichen Protestbezeugungen beigetragen haben.

Während der Innenminister seinen Kritiker lautes Geschrei aus Unverständnis und mangelnde Kenntnis der Verfassung vorwirft, diese gleichzeitig aber ändern will, droht ihm die Unterstützung in der eigenen Fraktion teilweise wegzubrechen. Zumindest sieht der CSU-Landesgruppenchef Peter Ramsauer den CDU-Kollegen auf "einem ganz schmalen Grat" wandeln. Auf der einen Seite stehe "das ausgesprochen hohe Sicherheitsbedürfnis in der deutschen Öffentlichkeit". Auf der anderen Seite "der Schrecken davor, vom Staat bis in die letzte Ecke der Privatsphäre ausleuchtbar zu werden", sagte er der Münchner Abendzeitung.

Er müsse dabei bisweilen an die visionäre Schrift "1984" von George Orwell denken, begab sich Ramsauer für einen CSU-Politiker auf ungewöhnliche Pfade. "Das Erschreckende ist, dass sich die Begründung von heute absolut deckt mit der aus Orwells Roman, nämlich: Sicherheit durch Ausforschen des Bürgers." Es sei sehr genau abzuwägen, wie angemessen die Überwachung sei und aus welchen Anlass die Bürger bespitzelt würden. Er halte es "für zu weitgehend, wenn mit der präventiven Keule aller sicherheitstechnischer Mittel 82 Millionen Deutsche über einen Kamm geschert" würden. Ramsauer warnte: Nicht jeder dürfe "von vornherein" zu einem möglichen Kriminellen und Sicherheitsrisiko abgestempelt werden.

Parallel zu der Frankfurter Kundgebung verabschiedete der Länderrat der Grünen in Bremen den Antrag "Bürgerrechte im digitalen Zeitalter schützen". Während Schäuble gerade versuche, "im Wochentakt mit neuen Vorschlägen Raubbau" an den Grundfreiheiten zu betreiben, fordert die Oppositionspartei unter anderem eine klare Ablehnung sowohl der Vorratsdatenspeicherung als auch der geplanten heimlichen Online-Durchsuchung privater Festplatten auf PCs oder von Speicherplattformen im Internet. Die vorgeschlagenen Erweiterungen der Ermittlungsmethoden "gaukeln eine allumfassende Sicherheit vor, die es nicht geben kann", heißt es zur Begründung. Die Auseinandersetzung mit Terrorismus und organisierter Kriminalität dürfe nicht dazu führen, "dass wir die Errungenschaften des demokratischen Rechtsstaates leichtfertig opfern."

Konkret appellieren die Grünen etwa an die Regierungskoalition, sich prinzipiell von dem von ihr bislang unterstützten Vorhaben zur "umfassenden und verdachtsunabhängigen Totalprotokollierung" der elektronischen Kommunikation der gesamten Bevölkerung zu distanzieren. Eine derartige "Speicherorgie" und weit reichende Registrierung des Verhaltens der Menschen in Deutschland, die über 80 Millionen Bürger unter Generalverdacht stelle, sei inakzeptabel. (Stefan Krempl) / (jk/c't)

<http://www.heise.de/newsticker/meldung/88254>

16.04.2007 15:08

[B]Datenschützer gegen zentrales Bundesmelderegister [/B]

Der Berliner Datenschutzbeauftragte Alexander Dix hat Pläne für ein Bundesmeldegesetz und ein damit möglicherweise verknüpftes einheitliches Melderegister für alle Bundesbürger als "Rückfall in die Zeit des zentralen Einwohnerregisters der ehemaligen DDR mit seinen Personenkennzeichen" zurückgewiesen. Diese Vergangenheit sei bei der deutschen Einigung als unvereinbar mit dem Grundgesetz angesehen und deshalb abgeschafft worden, gibt Dix zu bedenken. Die dezentrale Verarbeitung von Meldedaten hat sich seiner Ansicht nach im vereinten Deutschland bewährt. Eine zentrale Datenhaltung dürfte dagegen Begehrlichkeiten nicht nur bei den Sicherheitsbehörden, sondern auch bei anderen öffentlichen Stellen und Unternehmen wecken. Der Polizei und den Geheimdiensten etwa würde bei zukünftigen bundesweiten Rasterfahndungen der Zugriff auf einen "riesigen Datenbestand" eröffnet.

Der Bund hat mit der Föderalismusreform die Gesetzgebungskompetenz für das Melderecht erhalten. Laut Dix laufen derzeit in Berlin Vorbereitungen für den Erlass eines Bundesmeldegesetzes, das die Länder auszuführen hätten. Dabei sei auch von der gefürchteten Schaffung eines Bundesmelderegisters die Rede, wodurch die Daten der 82 Millionen Einwohner der Bundesrepublik zentral erfasst würden. Selbst wenn keine zentrale Meldebehörde vorgesehen sei, könnte Dix zufolge die zunehmende Vernetzung der kommunalen Melderegister in der Praxis ohne den Einbau zusätzlicher Sicherungen und Zugriffshürden zu einer zentralisierten Datenverarbeitung und einem gemeinsamen Informationsbestand führen.

Die zentrale Datenhaltung beziehungsweise Vernetzung der Meldestellen soll den Bürgern nach Angaben des Datenschützers mit den Schlagworten "E-Government" und "größere Bürgernähe" schmackhaft gemacht werden. Die sei allerdings nur gegeben, wenn die Betroffenen selbst darüber entscheiden dürften, ob Meldebehörden ihre personenbezogenen Informationen stärker als bisher austauschen könnten.

Dix bringt den Vorstoß aus Reihen der Bundesregierung in Zusammenhang mit dem vom Bundesinnenministerium geforderten, heftig umstrittenen Zugriff der Sicherheitsbehörden auf biometrische Daten aus RFID-bestückten Ausweisdokumenten. Diese Forderung aus Unionskreisen werde zu Recht von vielen Experten und einem Großteil des Bundestags abgelehnt. Das Vorhaben zur Schaffung eines Bundesmelderegisters dürfe hinter dem Wirbel um biometrische Zentraldateien aber nicht aus den Augen verloren werden.

Datenschützer sehen Personenkennciffrn, die dem Betroffenen anders als die Personalausweisnummer lebenslang und noch über sein Ableben hinaus angehaftet sowie mit umfangreichen Datenbeständen verknüpft werden können, seit Langem kritisch. Sie fürchten einen Einstieg in die Totalerfassung der Bevölkerung. Nichtsdestoweniger hat der Bundesrat bereits im November einem Verordnungsentwurf der Bundesregierung zur Einführung einer eindeutigen und dauerhaften Identifikationsnummer für Besteuerungsverfahren zugestimmt.

Alle Bundesbürger vom Baby bis zum Greis erhalten so vom Juli an vom Bundeszentralamt für Steuern eine Personenkennciffer zugeteilt. Die bislang dezentral geführten Datenbestände der über 80 Millionen in Deutschland gemeldeten Personen aus rund 5300 Meldestellen werden gleichzeitig erstmals zentral bei der dem Bundesfinanzministerium angegliederten Behörde zusammengeführt. Ersetzt werden dabei die noch von Land zu Land verschieden angelegten bisherigen Steuernummern. Der "gläserne Bürger" werde mit dieser ID und den bereits etablierten Kontroll- und Abfragemöglichkeiten Realität, warnt der Bund der Steuerzahler. (Stefan Krempl) / (pmz/c't)

<http://www.heise.de/newsticker/meldung/88305>

16.04.2007 19:31

[B]Schäuble will Leitlinien für innere Sicherheit erarbeiten [/B]

Bundesinnenminister Wolfgang Schäuble (CDU) will erstmals "Leitlinien für die innere Sicherheit" vorlegen. Das Grundsatzpapier soll bis zur zweiten Jahreshälfte fertig sein, bestätigte ein Ministeriumssprecher am heutigen Montag in Berlin. Vor dem Hintergrund der terroristischen Bedrohung will Schäuble die Trennung zwischen äußerer und innerer Sicherheit aufheben. Der neue Sicherheitsbegriff stößt bei der SPD auf Widerstand. Auch die heftige Debatte über Schäubles Sicherheitspolitik geht weiter.

Wie die Zeitung Die Welt berichtet, will Schäuble den auch in der großen Koalition umstrittenen Einsatz der Bundeswehr im Inneren in einem neuen Sicherheitskonzept festschreiben. "Wir wollen einen umfassenden Sicherheitsbegriff zu Grunde legen. Daher werden wir über die völlig überkommene Trennung von innerer und äußerer Sicherheit zu reden haben und die Frage eines Einsatzes der Bundeswehr im Inneren", sagte Schäuble dem Blatt. "Uns leitet die folgende Frage: Was muss man tun, um trotz vieler Gefahren den Menschen ein möglichst großes Maß an Sicherheit zu gewährleisten?"

Der innenpolitische Sprecher der SPD-Bundestagsfraktion, Dieter Wiefelspütz, warnte den Minister vor einem Alleingang. "Schäuble ist gut beraten, rechtzeitig mit dem Koalitionspartner zu sprechen, sonst wird es bei einer bloßen Ankündigung von Leitlinien bleiben", sagte Wiefelspütz der Netzeitung. Er lehnte Schäubles Sicherheitsbegriff und einen Einsatz der Bundeswehr im Inneren ab.

In der Diskussion über die von Schäuble geplanten schärferen Sicherheitsgesetze werben die Grünen für einen gemeinsamen Widerstand der Opposition. Grünen-Chef Reinhard Bütikofer sagte, es gehe um so viel, "dass wir dafür werben, dass hier alle, denen der Rechtsstaat lieb und teuer ist, an einem Strang ziehen, um zu verhindern, dass Herr Schäuble damit durchkommt". Insbesondere kritisierte Bütikofer die geplanten heimlichen Online-Untersuchungen von Computern.

Die innenpolitische Sprecherin der FDP-Bundestagsfraktion, Gisela Piltz, sagte, Schäubles Vision von einem umfassenden Sicherheitsbegriff und die erneute Ankündigung, Militär im Inneren einzusetzen, klängen wie eine Drohung. "Wolfgang Schäuble lässt einfach nicht locker und ist dabei, sich vollends zu verrennen." Piltz forderte die Kanzlerin auf, den Innenminister zu stoppen. Die stellvertretende Vorsitzende der Links-Fraktion, Petra Pau, warf Schäuble vor, Sicherheit notfalls auch über das Grundgesetz zu stellen.

Unionspolitiker verteidigten hingegen Schäuble. CSU-Generalsekretär Markus Söder befürwortete im Fernsehsender Phoenix eine Ausweitung der Sicherheitsgesetze. Die CDU-Innenpolitiker Clemens Binninger und Ralf Göbel wiesen die Kritik an Schäuble als überzogen zurück. Binninger verteidigte den Vorstoß Schäubles, über das Internet auf die Computer verdächtiger Personen zugreifen zu können. Es werde immer noch unterschätzt, welche Bedeutung das Internet für Terroristen und Kriminelle habe.

<http://www.heise.de/newsticker/meldung/88326>

LuCk3R - 19.4.2007 um 19:29

<http://www.godofgta.de/panopti/swf/index.htm>

Auch eine ziemlich aufschlussreiche Seite, die gerade denen die immer denken "Ich hab doch nichts zu verbergen!" die Augen öffnet. Vor allem findet man dort Informationen über die alltäglichsten Überwachungsmethoden.

Hansi - 19.4.2007 um 19:42

aha, postet der lucker hier endlich mal mit, ja!?! brav ☐

LuCk3R - 19.4.2007 um 19:47

Zeit wird's ja allemal.

jan91 - 19.4.2007 um 22:30

dabei ist zeit doch angeblich eine ressource, die dir nicht so oft zur verfügung steht^^

egal, dafür kommste halt einmal mathe weniger (würd ja nicht auffallen^^) und postet mal n bischen in der unity rum^^

Hansi - 20.4.2007 um 13:05

na dann mal herzlich willkommen in der unity @lucker ☐.
