Überwachung - Onlinedurchsuchungen

Reizthemen unserer Zeit ...

von Joachim Jakobs

Die Bundesrepublik auf dem Weg zum (käuflichen?) Überwachungsstaat?

"*Die Bürger müssen den Staat kontrollieren und nicht der Staat die Bürger*", so fasste ein Teilnehmer der Veranstaltung privatsphaere.org Mitte Dezember die Stimmung unter den rund 80 Anwesenden in Mannheim zusammen.

Was steckt hinter der "Onlinedurchsuchung"

Die technischen Möglichkeiten der Kontrolle durch den Staat stellte Constanze Kurz von der Humboldt-Universität zu Berlin in ihrem Vortrag vor: So verharmlost ihrer Meinung nach der Begriff "Onlinedurchsuchung" die Möglichkeiten der Sicherheitsbehörden. Denn schließlich seien viele Computer heute mit Mikrofon und Kamera ausgestattet. Deshalb sei der Begriff "Computerwanze" treffender. Mit ihr ließe sich nämlich der Wohn- oder Büroraum sowohl optisch als auch akustisch überwachen. Außerdem weist sie auf den Zusammenhang zwischen dieser Wanze und dem "Hackerparagraphen" [1] 202c Strafgesetzbuch (StGB) hin.

Dieses Gesetz stellt Software unter Strafe, mit der Unternehmen die Sicherheit ihrer Firmennetze prüfen, da mit derartiger Software auch Straftaten verübt werden könnten. Es sei bemerkenswert, daß der Staat einerseits drohe, privat und betrieblich genutzte Rechner auszuforschen und andererseits den Unternehmen praktisch zeitgleich verbieten würde, ihre Netze gegen virtuelle Eindringlinge zu sichern. Dies käme - so ein Teilnehmer - einem Berufsverbot für Informatiker gleich und könnte letztlich zur Auswanderung von Sicherheitsspezialisten führen. Sollte das passieren, würde der IT- Standort Deutschland nachhaltig geschädigt.

Ich hatte in dem Zusammenhang bedauert, daß der Branchenverband Bitkom sich nicht deutlich gegen die Absichten der Bundesregierung ausspreche, sondern lediglich "strenge Bedingungen" [2] fordert.

Ist die Kreditwürdigkeit gewerblicher Unternehmen gefährdet?

In seinem Beitrag knüpfte Bertold Roth, IT Verantwortlicher von "pro clima" - einem mittelständischen Baustoffhersteller, an Constanze Kurz an: pro clima sei ein forschungsintensives Unternehmen, das unter ständiger Beobachtung seiner Wettbewerber liege.

"Wenn Herr Schäuble uns nun durchsuchen kann, können unsere Wettbewerber das auch. Warum sollte eine Bank uns eine Neuentwicklung finanzieren, wenn sie damit rechnen müsste, daß unser Wettbewerber einfach so durch unser Netz spazieren kann und dann womöglich eine Woche vor uns beim Patentamt den Antrag stellt", fragt Roth.

Freie Software neigt zu „höherer Sicherheit"

Zwischendurch wies ich auf Gerüchte [3] hin, nach denen die Chinesen im Sommer bereits die Bundesregierung durchsucht hätten. Das Auswärtige Amt sei nicht durchsucht worden und das obwohl es mit hunderten von ausländischen Konsulaten und Botschaften vermutlich stärker gefährdet sei, als jede andere Deutsche Behörde. Womöglich liege der Grund dafür in der konsequenten Verfolgung einer IT Strategie auf Basis Freier Software [4]. Diese neige zu höherer Sicherheit, weil alle Sicherheitsspezialisten dieser Welt Verbesserungen beitragen könnten, während die Entwickler unfreier Software im Saft ihrer geschlossenen Gruppe schmorten.

Festzuhalten bleibt für mich: Der Staat befindet sich in einem Zielkonflikt: Wenn es die Chinesen nicht schaffen, eine Firma zu durchsuchen, schafft Herr Schäuble es vermutlich auch nicht.

Der Staat sollte sich bemühen, die Bürger zu schützen

Constanze Kurz verwies darüber hinaus auf das "Bundesamt für Sicherheit in der Informationstechnik" (BSI), das sich seit Jahren nicht nur um die Entwicklung von sicheren Systemen, sondern auch um die Entwicklung einer "Sicherheitskultur" in Deutschland bemühe. Dessen Bemühungen würden nun von seiner vorgesetzten Behörde, dem Bundesinnenministerium konterkariert:

"Die Bürger müssen jetzt dem Staat mißtrauen und damit rechnen, daß sie in ihrer elektronischen Steuererklärung oder einem anderen elektronischen Dokument ein Schadprogramm vom Staat untergejubelt bekommen". Auch in dieser Beziehung seien Anwender Freier Software besser vor Angriffen geschützt. Teilnehmer der Veranstaltung fürchteten daraufhin, daß der Staat womöglich Freie Software langfristig verbieten könnte.

Viele Unternehmen wähnen sich - zu Unrecht - in Sicherheit

Ein Teilnehmer - ein Unternehmer aus der Finanzwirtschaft und bekennender Anwender proprietärer Software - rief plötzlich aus: "Seit Jahren höre ich, in meiner Firma sei alles in Ordnung, und jetzt erfahre ich hier plötzlich, daß garnichts in Ordnung ist - was soll ich denn jetzt tun?" Eine wirklich befriedigende Antwort gab"s darauf allerdings nicht.

Allerdings scheint auch bei großen Unternehmen - beispielsweise aus der Bankwirtschaft - hier Fehleranzeige zu herrschen: So sind selbst Spitzeninstitute nach Teilnehmerangaben nicht in der Lage, elektronische Signaturen zu lesen, geschweige denn, ihre eigenen Emails zu verschlüsseln. Stattdessen würden den Kunden durchaus schützenswerte Kontoinformationen ohne jegliche Sicherung zugesandt.

Die elektronische Gesundheitskarte bedroht jeden Bürger

Mit seinen zahlreichen Aktivitäten scheint der Staat aber nicht nur die Wirtschaft, sondern auch die Privatsphäre und sogar die Gesundheit der Bürger selbst massiv zu bedrohen. Die Augenärztin Dr. Stephanie Gösele beschäftigte sich in ihrem Vortrag mit der elektronischen Gesundheitskarte (eGK) und konfrontierte die Versprechungen der Politik mit der Realität: So behaupte die Politik, die Patienten seien Herren über ihre Daten.

Tatsächlich bestünde das geplante Pseudonym der elektronischen Gesundheitskarte aus Geburtsjahr, Geschlecht, Versichertenstatus und Postleitzahl. Damit sei keine ausreichende Anonymität gegeben, so Gösele. Um den künftigen "morbiditätsorientierten Risikostrukturausgleich" unter den Krankenkassen berechnen zu können, sei es notwendig, jeden Patienten einer von sechs Risikoklassen zuzuordnen. Diese wirke dann "wie ein lebenslanger Stempel" und könne sich sogar noch - etwa bei erblichen Faktoren - negativ auf Kinder und Enkelkinder auswirken.

Die Augenärztin rät daher den Teilnehmern,

1. der Krankenkasse kein Foto zu schicken, denn ohne Foto keine eGK,
2. 2. kein Einverständnis zu den "Freiwilligen Anwendungen" zu erteilen und
3. 3. die alte Versichertenkarte zu behalten.

Ob sich dieses Verhalten nach der Gesetzeslage realisieren lassen wird, wird man dann sehen. Zumindest ist damit eine Signalwirkung verbunden, die sich mit dem vorhandenen Protest der Ärzteverbände summieren könnte.

Die Bundesrepublik auf dem Weg zum (käuflichen) Überwachungsstaat?

Ich zitierte im Anschluss daran aus einem Bericht [5] (PDF) der Gesellschaft für Informatik:

"Die gespeicherten Patientendaten können verknüpft werden mit den Daten aus Genomdatenbanken, der Mautdatenbank, den gespeicherten Verbindungsdaten der Telefongesellschaften, Bankkonten, Maut, Straßenkontrollen, Buchungsdaten von Flügen etc. Damit können Fragen gestellt werden wie: Wer wohnt in Köln, hat im letzten Jahr mehr als 25.000 verdient, war zweimal in den USA, fuhr mehr als 5-mal mit dem Auto nach Aachen, telefoniert wöchentlich mit München und leidet an Schwerhörigkeit und es wird eine Antwort geben."

Außerdem wies ich darauf hin, daß die Bundesregierung offenbar wenigstens mit dem Gedanken gespielt habe, die Daten aus dem biometrischen Personalausweis an die Wirtschaft zu verkaufen [6]. Und es gibt weitere Kritik [7] an der Gesundheitskarte.

Die Bürger sind sind zu sorglos

Der Rechtsanwalt und Mediator Dr. Thomas Lapp aus Frankfurt beschrieb die Gefahren von Vorratsdatenspeicherung und Onlinedurchsuchung aus rechtlicher Sicht und betonte, dass es nunmehr einen Generalverdacht gegen alle Bürger ohne Zusammenhang mit einer konkreten Straftat gebe.

Weiter erklärte er, dass bei Vorratsdatenspeicherung nur noch für Strafverteidiger, Abgeordnete und Geistliche ein umfassender Schutz besteht, während andere Rechtsanwälte, Ärzte sowie Beratungsstellen nur im Einzelfall geschützte Kommunikation anbieten können.

Dr. Lapp sieht allerdings nicht nur Gefahren in heutigem und künftigem Recht, sondern auch in der Sorglosigkeit der Bürger selbst und empfahl, "ein Bewusstsein dafür zu entwickeln, dass das Internet kein anonymes Medium ist und Daten, die heute dort gespeichert werden, noch in 10 Jahren über Suchmaschinen gefunden werden können".

Daher empfiehlt Lapp, bei Eintragungen im "Web 2.0" genau zu prüfen, ob man mit diesem Text, Bild oder sonstigen Angaben noch in zehn Jahren über Suchmaschinen gefunden werden will.

Weiterhin empfiehlt Lapp, Kommunikation per E-Mail durch Verschlüsselung und Signatur zu sichern und weist dazu ausdrücklich auf entsprechende Freie Software wie GnuPG hin. Ein Teilnehmer wies im Zusammenhang mit dem "Web 2.0" auf Überlegungen von StudiVZ [8] hin, die Daten seiner Anwender zu verkaufen.

Die Vorratsdatenspeicherung bedroht die Pressefreiheit

Der Journalist und Redakteur der Tageszeitung "Die Rheinpfalz" Thomas Huber beschäftigte sich aus journalistischer Sicht mit der Vorratsdatenspeicherung: Künftig wird jegliche Telekommunikation vom Staat aufgezeichnet - nicht der Inhalt, aber doch Beginn und Ende eines jeden Telefonats und die Teilnehmer; bei Mobilfunkgesprächen außerdem die Mobilfunkzelle, in der sich die Teilnehmer befinden. Im Internet werden Sender und Empfänger von E-Mails festgehalten und die aufgerufenen Webseiten protokolliert.

Huber ist sich sicher: "Die Informanten investigativ tätiger Journalisten werden sich gut überlegen, wem sie künftig welche Information zukommen lassen. Wir wissen aus der Psychologie: Menschen verhalten sich unter Beobachtung anders!" Außerdem fürchtet Huber, daß Informanten angesichts des künftigen Aufwands, ihre Spuren zu verwischen, auf die Idee kommen könnten, "das, was sie zu sagen hätten, sei doch eigentlich garnicht so wichtig". Auf diese Weise könnten den Medien wesentliche Informationen entgehen und die Pressefreiheit Schaden nehmen.

Ähnliche Erfahrungen liegen aus Belgien [9] bereits vor. Dort ist die entsprechende Direktive der Europäischen Union bereits umgesetzt. Ähnliche Erfahrungen wurden offenbar auch schon bei Sozialdiensten und Caritativen Einrichtungen gemacht: Betroffene von sexuellen Übergriffen etwa könnten sich kaum mehr anonym per Telefon "outen". Der freiberufliche Informatiker Arne Wichmann rief in seinem Vortrag dazu auf, Freie Software wie GnuPG [10] zu benutzen und die Vorgänge in der Politik einer breiten Bevölkerung bekannt zu machen.

Die Gesellschaft ignoriert die Gefahr

Allgemeine Ratlosigkeit herrschte bei Veranstaltern wie Publikum darüber, daß die Journalisten im Saal an einer Hand abzuzählen waren. Von der produzierenden Wirtschaft, den Anwälten, Steuerberatern, Heilberufen und Sozialdiensten war die Beteiligung noch geringer. "Diese Gesellschaft diskutiert ständig über Kindergeld und Benzinpreise, und die wirklich wichtigen Themen fallen völlig unter den Tisch", fasste ein Teilnehmer die Situation am Ende zusammen.

Hinweis zur Kampagne:

Der Lehrstuhl für Praktische Informatik I der Universität Mannheim - einer der Veranstalter der Initiative privatsphaere.org - wird die Videos der Vorträge noch vor Weihnachten auf den Server der Universität stellen. privatsphaere.org wird auf diese Videos verlinken. Gleichzeitig werden die Folien der Vorträge veröffentlicht.

Links zum Artikel:

[1]
http://de.wikipedia.org/wiki/Hackerparagraf

[2]
http://www.bitkom.org/de/presse/8477_49293.aspx

[3]
http://www.heise.de/newsticker/meldung/94980

[4]
http://www.germany.fsfeurope.org/documents/freesoftware.de.html

[5]
http://www.gi-ev.de/fileadmin/redaktion/Download/gi_thesen_gesundheitskarte050310_w.pdf

[6]
http://www.heise.de/tp/r4/artikel/21/21937/1.html

[7]
http://www.fsfe.org/en/fellows/jj/jj_s_blog/freie_software_fuer_freie_patienten

[8]
http://www.heise.de/newsticker/meldung/100642

[9]
http://www.heise.de/newsticker/meldung/96130

[10]
http://www.gnupg.org/(de)/index.html