Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft

Andreas Pfitzmann (Lehrstuhl Datenschutz und Datensicherheit, Fak. Informatik, TU Dresden)

V1.0, 26.09.2007

Zusammenfassung

Eine systematische Darstellung und Analyse der Möglichkeiten und Grenzen, wie der Gebrauch von Informations- und Kommunikationstechnik in einer freiheitlichen demokratischen Gesellschaft überwacht werden kann, ergibt:

Eine *Vorratsdatenspeicherung* sollte unterlassen werden, da sie eine bedeutende zusätzliche Sicherheitslücke schafft und ihr Übermaß eine gesellschaftliche Akzeptanz für andere, sehr viel zielgerichtetere und zweckgeeignetere Überwachungsmaßnahmen verhindert.

Falls eine *Online-Durchsuchung* in begründeten Fällen erlaubt werden soll, ist als Eindringmethode ausschließlich der „physische Zugriff auf das Endgerät“ zu erlauben.

Wo immer möglich, sollte statt einer Online-Durchsuchung eine *verdeckte Analyse der physischen Abstrahlung des Endgeräts* durchgeführt werden. Sie ergibt nur Erkenntnisse über die gegenwärtige Datenverarbeitung. Sollten Erkenntnisse über vergangene Datenverarbeitung benötigt werden, kann die verdeckte Analyse der physischen Abstrahlung des Endgeräts mit einer späteren offenen Beschlagnahme des Endgeräts kombiniert werden. Dies hat den Vorteil, dass die Beweiseignung der gewinnbaren Erkenntnisse so nicht zerstört wird.

Einführung

Abhörschnittstellen, Vorratsdatenspeicherung, Online-Durchsuchung, Video-Überwachung, Fingerabdruck-Biometrie in Reisepässe – der Staat rüstet auf mit dem Ziel, sich und seine Bürger zu schützen. Aber welche dieser Maßnahmen schützen die Bürger mehr, als dass sie sie gefährden? Welche dieser Maßnahmen stärken das Vertrauen und den Zusammenhalt innerhalb der Gesellschaft und zwischen Bürgern und Staat? Welche stellen dagegen wichtige Vertrauensverhältnisse in Frage und schwächen so die freiheitliche demokratische Gesellschaft?

Leider können auch wir Wissenschaftler nicht alle Fragen beantworten. Aber wir wollen einerseits dazu beitragen, dass keine wichtigen Fragen vergessen oder gar unterschlagen werden. Andererseits sind manche Antworten durchaus möglich – auch wenn sie manchen unbequem erscheinen mögen.

Zunächst wichtige Fakten

Informationstechnik (IT) hat in den letzten zwei Jahrzehnten eine Komplexität erreicht, mit der weder die Wissenschaft Informatik einschließlich der durch sie bereitgestellten Werkzeuge zum Entwurf und zur Analyse von IT noch unsere Fähigkeit, IT-Systeme zu betreiben, Schritt gehalten haben. Im Ergebnis sind heute viele IT-Systeme abenteuerlich unsicher – auch angeblich gut gesicherte IT-Systeme sind durch Fachleute erfolgreich angreifbar.

Kommunikationstechnik (KT) basiert zunehmend auf IT, so dass die Knoten der KT zur Übertragung von Daten durch Fachleute erfolgreich angreifbar sind. Werden Daten vor der Übertragung nicht verschlüsselt, sind sie also weitestgehend ungeschützt – gegenüber einem Zugriff auf den Knoten, die sie durchlaufen, wie auch auf den Kommunikationskanälen.

IT und KT wachsen zunehmend zur Informations- und Kommunikationstechnik (IKT) zusammen (d.h. multifunktionale Endgeräte verbunden durch Kommunikationstechnik), was die Unsicherheit steigert und immer mehr Akteuren erfolgreiche Angriffe ermöglicht.

Selbst bei größten Anstrengungen aller Beteiligten (insbesondere der IKT-Hersteller, Betreiber und Nutzer) wird eine rein marktgetriebene deutliche Verringerung der Unsicherheit von IKT etliche Jahrzehnte dauern. Um eine deutliche Steigerung der Sicherheit von IKT in überschaubaren Zeiträumen zu erreichen, wäre eine nur regulatorisch herbeiführbare, drastische Komplexitätsreduktion nötig, die unweigerlich mit einer Funktionsreduktion einherginge. Dies erscheint so wenig durchsetzbar, dass darüber nicht einmal nachgedacht wird.

Es ist zu erwarten, dass für weit verbreitete persönlich genutzte Endgeräte (u.a. alle Arten von Telefonen, PDAs, Laptops, Desktop-PCs) Eigentümer und Benutzer identisch sind (*Eigennutzer*) und diese Endgeräte u.a. aus marktwirtschaftlichen Gründen vorwiegend für die (Sicherheits-)Interessen ihrer Eigennutzer gebaut werden. Andernfalls wären sie schlicht unverkäuflich. Würde in Märkte regulatorisch eingegriffen, um Endgeräte anders zu gestalten, als dies die (Sicherheits-)Interessen ihrer Eigennutzer nahelegen, dann würden insbesondere Kriminelle und Terroristen sich solcher Endgeräte keinesfalls bedienen.

Da (Mobil-)Telefone, PDAs, Laptops und Desktop-PCs sich normalerweise in einem durch den Eigennutzer weitgehend kontrollierten physischen Schutzbereich befinden (je nach Lebensstil in Hemden- oder Jackettasche, Rucksack oder Aktenkoffer, Wohnung oder Büro), ist nicht zu erwarten, dass ihre Eigennutzer Wert auf Schutz gegen physische Eingriffe (tamper resistance) legen werden. Eher im Gegenteil, da physischer Schutz gegen sie selbst ihre Kontroll- und Nutzungsmöglichkeiten reduziert (Digital Rights Management, treffender Digital Restrictions Management ist bei Eigennutzern nicht gerade beliebt). Zu erwarten ist also, dass persönliche Endgeräte „von der Stange“ zunehmend gesichert werden gegen „logische“ Angriffe über Kommunikationsnetze, nicht aber gegen physische Angriffe. Dies liegt nicht nur an den gerade geschilderten Interessen an Autonomie der Eigennutzer und wirtschaftlichen Interessen der international tätigen Hersteller der Endgeräte, sondern auch an physischen Gründen: Schutz gegen physische Eingriffe macht Geräte schwerer und unhandlicher. Dieser allgemeine Trend schließt natürlich nicht aus, dass einzelne Eigennutzer ihr Endgerät mit Erkennungsmechanismen für physische Eingriffe (tamper detection) ausstatten, beispielsweise schwer nachmachbare und kaum lösbare Klebestreifen zur Sicherung der Öffnungsmöglichkeiten des Gehäuses anbringen.

Physische Gründe begrenzen auch den Schutz gegen physische Abstrahlung (TEMPEST). TEMPEST-Angriffe bezeichnen Methoden, mit denen von einem Gerät abgestrahlte elektromagnetische Wellen (z.B. von Tastatur oder Grafikkarte) aufgefangen und genutzt werden, um daraus die im Gerät momentan verarbeiteten Informationen (z.B. Tastatureingaben oder Bildschirminhalte) abzuleiten. TEMPEST-Angriffe verändern die im Gerät verarbeiteten Daten und Programme nicht. Selbst durch Inkaufnahme deutlichen Mehrgewichts ist Schutz gegen TEMPEST-Angriffe keinesfalls auch nur annähernd perfekt zu realisieren. Wegen der durch das Mehrgewicht deutlich geringeren Marktgängigkeit und zusätzlichem technischem Aufwand sind TEMPEST-geschützte Geräte deutlich teurer als entsprechende Geräte ohne TEMPEST-Schutz. Wer TEMPEST-geschützte Geräte kauft oder benutzt fällt also auch in der vorhersehbaren Zukunft auf.

Dienste wie z.B. E-Mail, die heutzutage noch über Server abgewickelt werden, so dass sie nicht nur in Endgeräten oder via physischer Abstrahlung in deren Nähe überwacht werden können, sondern auch in Servern, werden zunehmend Verschlüsselung der Nutzdaten verwenden, so dass diese Nutzdaten, z.B. die Inhalte der E-Mails, auch vor den Servern (und damit auch vor Überwachung der Server oder in den Servern) geschützt sind. Zusätzlich ist es mittels sogenannter Peer-to-Peer-Netzwerke (P2P) zunehmend möglich, Dienste ohne professionell betriebene Server anzubieten. Zusammen bedeutet dies, dass zukünftig Überwachung sinnvollerweise nicht an Servern ansetzt, sondern bezogen auf Nutzdaten ausschließlich am Endgerät und bezogen auf Verbindungsdaten („wer kommuniziert wann von wo mit wem wohin?“) hauptsächlich am Endgerät. Kommt es auf die Beweiseignung von Nutzdaten oder Verbindungsdaten an, ist darauf zu achten, dass Daten und Programme im Endgerät nicht zu Überwachungszwecken verändert werden [Hansen, Pfitzmann 2007].

Wichtige Grundsätze

1. Da die hoch entwickelte Gesellschaft auf IKT und damit um der Sicherheit der Gesellschaft willen auf sichere IKT sehr viel mehr angewiesen ist als die organisierte Kriminalität oder terroristische Netzwerke, sollte der Staat alles unterlassen, was die Entwicklung der IKT hin zu mehr Sicherheit erschwert und damit zumindest verzögert.

2. Bei aller IKT für staatliche Sicherheitszwecke (Abhörschnittstellen, Datenbanken der Sicherheitsbehörden, Vorratsdatenspeicherung bei KT-Betreibern) muss man sich bewusst sein, dass auch diese IKT nicht wirklich sicher betrieben werden kann, solange die IT-Basissysteme derart unsicher sind, wie dies für wenigstens die nächsten zwei Jahrzehnte, vermutlich deutlich länger, zu erwarten ist. Im Klartext bedeutet das, dass keineswegs nur Partner-Geheimdienste, sondern auch solche von sogenannten Schurkenstaaten sowie die organisierte Kriminalität und auch terroristische Netzwerke sehr gute Chancen haben, sich „unserer“ – für staatliche Sicherheitszwecke vorgesehenen – IKT zu bedienen. Dies gilt insbesondere selbst dann, wenn unsere Sicherheitsbehörden organisatorisch perfekt geführt würden und es bei ihnen, was eine historische Weltneuheit wäre, weder Doppelagenten noch irgendwelche Korruption oder Erpressbarkeit gäbe. Also muss IKT für staatliche Sicherheitszwecke zumindest für die nächsten Jahrzehnte sehr vorsichtig geplant und eingesetzt werden.

3. Der Staat sollte also die Entwicklung hin zu wirklich sicherer IKT fördern. Und dies bedeutet auch, dass diese IKT tendenziell auch gegenüber dem Staat sicher sein muss, zumindest solange 2. aus technischen Gründen gilt. Da auch staatliche

Sicherheitsorgane aus fehlbaren Menschen bestehen, gilt diese Aussage vermutlich zeitlich uneingeschränkt.

4. Da Kriminelle, Terroristen wie auch fremde Geheimdienste Sicherheitslücken bestehender IKT nutzen, sollte dies durch einen geeigneten (grund-)gesetzlichen Rahmen auch unseren Bedarfsträgern eher erlaubt werden, als dass für sie zusätzliche Sicherheitslücken geschaffen werden. Dabei muss sehr darauf geachtet werden, dass unsere Bedarfsträger kein Interesse an der Konservierung der von ihnen mitgenutzten Sicherheitslücken entwickeln oder diesem Interesse zumindest keine Geltung verschaffen können.

5. Schon heute werden auf eigengenutzten Endgeräten persönlichste Informationen gespeichert (Tagebücher, privateste Gedanken, Notizen, ...). Diese müssten bei einer Durchsuchung konsequenterweise auch ausgewertet werden, da bei jeder Beschränkung der Durchsuchung auf einen wie auch immer gearteten Teilbereich zum Schutz des Kernbereichs privater Lebensgestaltung dies zum Verbergen ermittlungsrelevanter Information genutzt werden kann. Also muss die Hürde für die Zulässigkeit einer Online-Durchsuchung mindestens so hoch gelegt werden wie für eine akustische Wohnraumüberwachung.

6. IKT für staatliche Sicherheitszwecke sollte so gestaltet werden, dass Kriminelle und Terroristen ihr nur sehr aufwändig ausweichen können – insbesondere sollte organisierten Kriminellen und allen Terroristen hierbei Intelligenz und Sachkunde unterstellt werden.

Erste Schlussfolgerungen

Wegen 1., 2. und 6. ist eine umfassende Vorratsdatenspeicherung sicherheitstechnisch schlicht abenteuerlich: Sie schafft deutliche Risiken für brave Bürger. Intelligente Kriminelle und Terroristen werden u.a. Anonymisierungsdienste im Ausland außerhalb der Vorratsdatenspeicherungsbereiche nutzen um sich selbst zu schützen. Selbst wenn diese Anonymisierungsdienste über unveröffentlichte Sicherheitslücken (*Less than zero day exploits*) [Pohl 2007] der zugrunde liegenden IT angreifbar sind, so kann deren Angreifbarkeit über minimale Installation von Funktionalität (Anonymisierungsknoten brauchen bei weitem nicht alle Dienste, die „normale“ Endgeräte heutzutage so leicht angreifbar machen) sowie physische Verteilung und Diversität (unterschiedliche Betriebssysteme, etc.) bereits heute so deutlich reduziert werden, dass sie für praktische Ermittlungen kaum eine Rolle spielen dürften.

Unter Beachtung von 4. kann eine verdeckte Online-Durchsuchung angemessen sein, wenn sich alle Beteiligten der Schwierigkeiten und Risiken bewusst sind und insbesondere Konsens darüber besteht, dass sie nur zur Indiziengewinnung zur Steuerung von Ermittlungen, wegen mangelnder forensischer Beweiskraft ihrer Ergebnisse aber nicht zur Beweiserhebung geeignet ist [Hansen, Pfitzmann 2007]. Wegen 5. muss die Zulässigkeit der verdeckten Online-Durchsuchung auf die Prävention schwerwiegendster Verbrechen beschränkt werden.

Für Erfolg und Angemessenheit einer verdeckten Online-Durchsuchung wie auch für ihr Missbrauchspotential ist die *Eindringmethode* wesentlich. Zunächst sind folgende Optionen denkbar [Hansen, Pfitzmann 2007]:

a) Methoden, die *unbewusste konstruktive Mitarbeit* desjenigen erfordern, dessen Endgerät durchsucht werden soll. Beispiele sind das Zusenden von E-Mails, die als Attachment ein Trojanisches Pferd enthalten, zu dessen Start der Eigennutzer verführt werden soll, oder das Zuspielen präparierter Datenträger.
b) Verpflichtung von Internet-Service-Providern, einen Programm-Download desjenigen, dessen Endgerät durchsucht werden soll, so zu modifizieren, dass das heruntergeladene Programm ein Trojanisches Pferd enthält.
c) Hacken des Endgeräts durch Ausnutzen von Sicherheitslücken, die noch nicht allgemein bekannt sind (*Less than zero day exploits*) [Pohl 2007].
d) Erreichen des *physischen Zugriffs auf das Endgerät* (sei es durch „Ausleihen" eines Mobiltelefons, Einstiegs in eine Wohnung zum Zugriff auf Desktop-PCs oder auf dort befindliche PDAs und Laptops), Kopieren seines Speichers, ggf. Maßschneidern einer Online-Durchsuchungs-Software für genau die vorgefundene Softwarekonfiguration, Einbringen der Online-Durchsuchungs-Software, ggf. bei einem zweiten „Ausleihen" oder Wohnungseinstieg [Leipold 2007].

Die Anwendung von Eindringmethode b) lässt sich durch eine leichte Erweiterung der heute üblichen Sicherheitsmechanismen beim Download von Software entdecken – und damit wirkungslos machen. Hierzu müssen nur viele Endgeräte miteinander Hashwerte ihrer Downloads austauschen, um Inkonsistenzen zu entdecken und bei entdeckten Inkonsistenzen auch die Downloads selbst auszutauschen[1]. Diese Entdeckung und Vereitelung funktioniert selbst dann, wenn der Hersteller des Programms rechtlich zur Kooperation verpflichtet wäre, indem er eine digitale Signatur unter sein um das Trojanische Pferd erweiterte Programm liefert. Damit solch eine Konsistenzprüfung leer läuft, müssten Programm-Downloads sich generell unterscheiden oder alle Nutzer (und damit in konsistenter Weise weltweit) ein Trojanisches Pferd enthalten. Ersteres ist technisch nicht plausibel[2]. Letzteres verstößt so eklatant gegen 3. und vermutlich auch gegen internationales Recht, dass sich eine weitere Diskussion erübrigt.

Da a), b) und c) zwar einen Grundaufwand zum Bereitstellen des Trojanischen Pferdes bzw. Know-hows erfordern, danach aber weitgehend ohne große Kosten im jeweiligen Anwendungsfall eingesetzt werden können, haben sie ein sehr großes Missbrauchspotential: Bei der Programmierung Trojanischer Pferde ist dies evident – sie können, wenn vorhanden, massenhaft eingesetzt werden, zumindest solange Endgeräte mit Softwarekonfigurationen „von der Stange" (d.h. wie als Komplettsystem gekauft) durchsucht werden sollen. Gleiches gilt für eine Infrastruktur zum Einfügen von Trojanischen Pferden in Downloads. Zum Finden von *Less than zero day exploits* wird eine bereits jetzt vorhandene „Szene" noch weiter ermuntert und monetär unterstützt – und sie wird nicht nur an deutsche Bedarfsträger verkaufen.

[1] Sollten Hersteller den Austausch der Downloads selbst verbieten (wie dies bei Microsoft wohl momentan der Fall ist), dann ist dies, zusammen mit der in diesem Papier diskutierten Bedrohung, ein sehr gutes Argument für die Verwendung von Open Source-Software. Außerdem werden organisiert Kriminelle und Terroristen solch ein Verbot vermutlich nicht befolgen.

[2] Selbst wenn Programm-Downloads etwa bei Update-Funktionen jeweils für die installierte Version maßgeschneidert werden, gibt es immer noch im Vergleich zur Zahl der Downloads wenige Varianten, so dass der beschriebene Mechanismus zur Konsistenzprüfung funktioniert.

Eindringmethode d) gibt der Online-Durchsuchung ein deutlich geringeres Missbrauchspotential, da sie wirklich einen deutlich spürbaren Aufwand in jedem einzelnen Anwendungsfall verursacht. Hierbei kommt es nicht auf das Maßschneidern der Online-Durchsuchungs-Software für die vorgefundene Softwarekonfiguration an – das ließe sich aus Sicht der Informatik gut automatisieren und damit bei Masseneinsatz nahezu beliebig billig pro Einsatz gestalten –, sondern auf den aufwendigen physischen Zugriff auf jedes einzelne Endgerät.

Wegen 3. ist die Möglichkeit der verdeckten Online-Durchsuchung mit den Eindringmethoden a), b) und c) ein Auslaufmodell: Je sicherer die Endgeräte werden, desto aufwendiger werden diese drei Eindringmethoden, bis sie bei wirklich sicherer IKT schließlich unwirksam werden. Auch dies spricht dafür, sich auf Eindringmethode d) zu beschränken und auch zu konzentrieren.

Wegen 6. vorzuziehen gegenüber einer verdeckten Online-Durchsuchung ist eine *verdeckte Analyse der physischen Abstrahlung des Endgeräts*.

- Ihr können sich Kriminelle und Terroristen auch langfristig kaum entziehen (s.o.), insbesondere auch nicht dadurch, dass sie ihr Endgerät nur offline betreiben (also beispielsweise ihren PDA, Laptop oder Desktop-PC nie ans Internet anschließen) oder mit Erkennungsmechanismen für physische Eingriffe versehen.
- Ihr deutlich spürbarer Aufwand in jedem einzelnen Anwendungsfall schließt einen Missbrauch durch massenhaften Einsatz aus.
- So gewonnene Erkenntnisse sind forensisch als Beweismittel verwertbar – im Gegensatz zu Erkenntnissen, die durch eine Online-Durchsuchung, egal mit welcher Eindringmethode, gewonnen wurden, da bei der Online-Durchsuchung das Endgerät immer manipuliert wird [Hansen, Pfitzmann 2007].
- Sie kann ggf. ergänzt werden durch eine später durchgeführte Beschlagnahme des Endgerätes und der auf ihm gespeicherten Daten, die etwa mittels der per Tastatureingabenaufzeichnung in Erfahrung gebrachten kryptographischen Schlüssel entschlüsselt werden können. Da bei diesem Vorgehen keine Manipulationen an den Daten oder Programmen auf dem Endgerät durchgeführt werden, sind die Ergebnisse forensisch als Beweismittel verwertbar.

Sowohl die Online-Durchsuchung mit Eindringmethode d) „physischer Zugriff auf das Endgerät“ wie auch die verdeckte Analyse der physischen Abstrahlung des Endgeräts stellen Maßnahmen mit lokal begrenzter Wirkungsentfaltung dar und passen so deutlich besser zu unserem Rechtssystem: Internationale Verwicklungen etwa durch Verstöße gegen das Völkerrecht bei unbeabsichtigtem „Auslandseinsatz“ werden vermieden; die Maßnahmen werden zielgerichteter und sind deutlich weniger missbrauchsgeeignet.

Empfehlungen

Von einer *Vorratsdatenspeicherung* sollte politisch abgerückt werden, da sie eine bedeutende zusätzliche Sicherheitslücke schafft und ihr Übermaß eine gesellschaftliche Akzeptanz für andere, sehr viel zielgerichtetere und zweckgeeignetere Überwachungsmaßnahmen verhindert.

Falls eine *Online-Durchsuchung* in begründeten Fällen erlaubt werden soll, ist als Eindringmethode ausschließlich der „physische Zugriff auf das Endgerät“ zu erlauben.

Wo immer möglich, sollte statt einer Online-Durchsuchung eine *verdeckte Analyse der physischen Abstrahlung des Endgeräts* durchgeführt werden. Sie ergibt nur Erkenntnisse über die gegenwärtige Datenverarbeitung, was für ihren kontrollierbaren Einsatz verglichen mit der Online-Durchsuchung ein großer Vorteil ist. Sollten Ermittlungserkenntnisse über vergangene Datenverarbeitung benötigt werden, kann die verdeckte Analyse der physischen Abstrahlung des Endgeräts mit einer späteren offenen Beschlagnahme des Endgeräts kombiniert werden. Dies hat den Vorteil, dass die Beweiseignung der gewinnbaren Erkenntnisse so nicht zerstört wird.

Danksagung

Für hilfreiche Diskussionen zu diesem Text danke ich Stefan Berthold, Rainer Böhme, Sebastian Clauß, Rüdiger Dierstein, Marit Hansen, Markus Hansen, Prof. Dr. Hartmut Pohl, Dr. Manfred Reitenspieß und Dr. Dagmar Schönfeld herzlich.

Literatur

[Leipold 2007] Roman Leipold: Der Bundestrojaner ist eine Wanze; Chip 09/2007 http://www.focus.de/digital/computer/chip-exklusiv/chip-exklusiv_aid_68603.html (20. Sept. 2007). (Authentizität der Aussagen wurde vom BKA dementiert http://www.ftd.de/forschung_bildung/forschung/238034.html?mode=print (20. Sept. 2007))

[Hansen, Pfitzmann 2007] Markus Hansen, Andreas Pfitzmann: Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme; Deutsche Richterzeitung, August 2007, Seite 225-228.

[Pohl 2007] Hartmut Pohl: Zur Technik der heimlichen Online-Durchsuchung; DuD Datenschutz und Datensicherheit 31 (September 2007) Seite 684-688.