RUBIKON

Samstag, 06. Oktober 2018, 15:57 Uhr
~15 Minuten Lesezeit

Der tiefe IT-Staat

Die Bürger werden belogen, betrogen, ausgeforscht und manipuliert.

von Wolfgang Romey
Foto: Gorodenkoff/Shutterstock.com

Die Annahme, dass es etwas nicht gibt, wenn man es nicht sieht, ist leider falsch. Es ist eine der gefährlichen Eigenschaften der IT-Technik, dass man ihr Wirken und ihre Auswirkungen meist nicht wahrnehmen kann. Das gilt auch für die fünf IT-Netze, die das Land und seine Bürger überziehen und mit deren Hilfe die Handelnden des tiefen IT-Staates die Bürger ausforschen, überwachen und beeinflussen.

Die fünf tiefen IT-Netze

Die Netze sind:

- das persönliche Mitnehm-Netz;
- das Netz im privaten Raum;
- das Netz im öffentlichen Raum;
- das Anwendungsnetz;
- das Netz der Geheimdienste.

Die Netze überschneiden sich teilweise, wirken aber erfolgreich zusammen. Genutzt werden die Netze von privaten und staatlichen Stellen, in der Regel im tief Verborgenen.

Das tiefe persönliche Mitnehm-Netz

Digitale Geräte, die die Nutzer immer bei sich tragen können, haben sich in den letzten Jahren rasant verbreitet. In erster Linie sind es Smartphones, fast alle Erwachsenen tragen eines bei sich, aber auch immer mehr Kinder und Jugendliche nutzen sie. Nicht ganz so verbreitet sind Tablets. Neu hinzugekommen sind „Fitness-Bänder“ und Automobile, die auch mit dem Internet verbunden sind.

Die Fitness-Bänder dienen dazu, den Gesundheitszustand der Nutzer zu erfassen und seine Bemühungen um dessen Erhalt und Verbesserung zu verfolgen. Bei den Autos ist es inzwischen möglich, das Fahrverhalten und die gefahrene Strecke zu erfassen. Die von Bändern und Autos jeweils erfassten Daten gehen mindestens an die Versicherungswirtschaft und bei Autos auch an die Automobilhersteller, ohne dass die Nutzer bemerken, wann das geschieht und welche Daten übertragen, wo gesammelt und gegebenenfalls weitergegeben werden. Erst wenn die Versicherungswirtschaft einen neuen Vertrag anbietet oder eine

Verbesserung der Versicherungsbedingungen verweigert, tritt das an die Oberfläche. An der Oberfläche sichtbar wird es auch, wenn auf Grundlage der Daten zukünftig die Schuldfrage bei Unfällen geklärt wird oder Strafen beispielsweise für Geschwindigkeitsübertretungen ausgesprochen werden. Unter der Oberfläche bleibt, wer die gefahrene Strecke wann aufzeichnet. Der Fahrer wird über sein Smartphone identifiziert. Die Teilnahme an einer kritischen Aktion ist damit kaum noch abzustreiten. Das alles geschieht, ohne dass es die Nutzer bewusst wahrnehmen, also tief verborgen.

Smartphone: mehr Überwachung geht nicht

Im Vergleich zu dem, was mit den Smartphones möglich ist und geschieht, ist das alles aber noch harmlos. Kein anderes digitales Gerät forscht den Nutzer so umfassend aus wie das Smartphone: Kontakte – damit auch den Bekanntenkreis des Nutzers –, Verbindungsdaten, seit neustem Inhalte von Telefongesprächen, gesprochenes Wort, einschließlich der Erkennung des Inhalts, Medien – Töne, Bilder, Filme –, E-Mails, Daten von Messengern, Nutzung sozialer Netzwerke, Surfverhalten sowie Ortsdaten über GPS und Telefonnetze. Von all dem bekommt der Nutzer in der Regel nichts mit. Es entsteht ein umfassender Datenschatten des Nutzers, in den Daten eingeflossen sind, die teilweise Jahrzehnte zurückreichen können.

Ein Beispiel: Während der Nutzer eine App verwendet, in einem Sozialen Netzwerk unterwegs ist oder surft, werden in Echtzeit Daten erhoben und an Anbieter von Werbung weitergeleitet. Diese Daten werden daraufhin abgeglichen und führen zu einem Angebot für einen Werbeplatz auf der genutzten Seite. In einer Art Auktion wird innerhalb von etwa 100 Millisekunden vom Seiten-Anbieter

entschieden, wer den Zuschlag für den Werbeplatz erhält. Der Nutzer wundert sich vielleicht nur, warum er schon wieder Werbung erhält, die so gut zu seinen Interessen passt (1).

> ***Selbstverständlich sind es nicht nur die Anbieter und Käufer von Werbeplätzen, die derartige Verfahren ausnutzen, für Behörden und Geheimdienste ist das natürlich gleichfalls möglich. Dem Nutzer bleibt völlig verborgen, wer welche Daten sammelt, verarbeitet, verkauft oder für Überwachung und Beeinflussung einsetzt.***

Das tiefe IT-Netz im privaten Raum: Verwanzen von Wohnungen war gestern

Das tiefe Netz im privaten Raum ist in den letzten Jahren rasant gewachsen und wächst ebenso schnell weiter. Die digitalen Geräte aus dem Internet of Things (IoT) sind hierbei ein wesentlicher Bestandteil. Sie werden von den Bewohnern der Wohnungen selbst gekauft und haben Eigenschaften, die eine Verwanzung überflüssig machen. Ans Internet angeschlossene Heizungen, Kühlschränke, Lampen, Jalousien, Fernseher – alles ist vernetzt; und damit nicht nur von den Wohnungs-Bewohnern von außen erreichbar. Sie sind ebenso angreifbar. Angreifbar nicht nur von Kriminellen, sondern auch von staatlichen Diensten, die nicht nur den Inhalt des Kühlschranks abgreifen. Da beispielsweise Lampen oder Fernseher auch Kameras enthalten können, kann in Abstimmung mit den Daten vom Smartphone festgestellt werden, wer wann in der Wohnung war.

Ist auch noch ein „smarter“ Lautsprecher vorhanden, können die Gespräche aufgezeichnet und die Inhalte entschlüsselt werden. Die Frage, ob es ein harmloser Freundeskreis war, der sich getroffen

hat, oder ein politisches Treffen, ist damit leicht zu beantworten. Praktischerweise stehen über die Smartphones der Teilnehmer auch deren Terminkalender, Daten der Kontakte, die empfangenen und versendeten E-Mails und die geführten Telefonate zur Verfügung. Wer will, kann sich ein differenziertes Bild von der Gruppe machen und gegebenenfalls einschreiten. Selbstverständlich wieder, ohne das die Teilnehmer das bemerken.

Besonders beliebt und perfide sind die von Amazon oder Google angebotenen smarten Lautsprecher. Da sie ununterbrochen auf den gesprochenen Befehl zur Aktivierung lauschen – „Alexa, gib meine Daten an den Verfassungsschutz“ – hören sie jedes gesprochene Wort mit, gleichen über das Internet die Stimmen mit den vorhandenen Daten ab oder versuchen, noch unbekannte Sprecher zu identifizieren. Da die Spracherkennung rasante Fortschritte macht, sind die Inhalte der Gespräche nach kurzer Zeit bekannt. Werden diese Themen dann beispielsweise mit den vom smarten Fernseher ermittelten Sehgewohnheiten abgeglichen, kann leicht Repressionsbedarf oder Erpressungspotenzial erkannt werden. Jeder, der eine Wohnung betritt, die nicht seine eigene ist, sollte sich erkundigen, welche „smarten“ Geräte gerade aktiv sind. Diese Datensammlung findet wie beim Mitnehm-Netz ohne das Wissen der Bewohner und Gäste statt; auch weil es ihnen meistens gleichgültig ist.

Das tiefe IT-Netz im öffentlichen Raum: Ausspähung hier und überall

Das tiefe IT-Netz im öffentlichen Raum tritt mit einigen Knoten an die Oberfläche: die allgegenwärtigen Überwachungskameras gehören dazu. In der Vergangenheit haben die Kameras nur Bilder aufgenommen und wiedergegeben. Menschliche Beobachter waren notwendig, um Auffälligkeiten zu erkennen. Das hat sich drastisch

geändert: Gesichtserkennung ist inzwischen fast Alltag, Lippenlesen auf dem Weg dorthin. Damit ist es inzwischen möglich, den Weg von Personen zu verfolgen und Gespräche abzuhören. Auch hier ergänzt das Smartphone die Möglichkeiten. Im Vergleich zu früher finden sich Überwachungskameras mit den wachsenden Fähigkeiten an wesentlich mehr Orten: in Kaufhäusern, Bussen, Straßenbahnen, Zügen, Hotels, …

Durch den Umbau der Städte zu „Smart-Cities“ wird sich das alles noch deutlich ausweiten: Straßenlampen, die Einwohner über das Smartphone, Kameras und über Mikrophone tracken, Straßenbahnen und Busse, die die Wege der Fahrgäste aufzeichnen, Erfassung der Bewegungen im geschlossenen öffentlichen Raum, Erfassung der Einkäufe durch Kreditkarten oder Paybackkarten. Es wird in naher Zukunft möglich sein zu erfassen, wer sich wohin begibt, mit wem er sich trifft, was die Gegenstände der Unterhaltungen sind. Vergessen sie die Möglichkeit anonym an einer Demonstration teilnehmen zu können oder sie unbeobachtet vorbereiten zu können. Im Unterschied zu den ersten beiden Netzen haben die Menschen hier wenig Möglichkeiten, sich diesem tiefen Netz zu entziehen.

Das tiefe IT-Anwendungsnetz

Die IT-Landschaft, nicht nur in Deutschland, ist geprägt durch die fast vollständige Abhängigkeit von den US-Konzernen Google und Microsoft. Google ist nahezu Monopolist bei den mobilen Geräten: Auf mindestens 80 Prozent der Geräte läuft das Google-Betriebssystem Android, die Anwendungen kommen bei diesen Geräten zu fast 100 Prozent aus dem Google-Playstore, in dem die Zulassung von Apps von Google abhängt und aus nichtigen oder willkürlichen Gründen gesperrt werden kann, wie sich erst kürzlich (2) wieder zeigte. Das Ausforschen der Nutzer hinter ihrem Rücken

durch die Apps ist selbstverständlich kein Grund für eine Sperrung. Klassisch ist die Taschenlampen-App, die sich umfassenden Zugang zu Kamera, Mikrophon oder Kontakten der Nutzer verschafft, um unter anderem Werbung zu platzieren.

Bei Desktop-Computern und Laptops sieht es nicht besser aus. Der US-Konzern ist nur ein anderer: Microsoft. Auf mehr als 90 Prozent dieser Geräte laufen das Betriebssystem Windows und die Bürosoftware Office.

Ein nicht unwesentlicher Aspekt dabei ist, das Microsoft regelmäßig durch viele Millionen auch aus Steuermitteln gezahlter Lizenzgebühren faktisch subventioniert wird.
Nicht nur bei privaten Nutzern: Behörden, Unternehmen, der Bildungsbereich, Museen, Gewerkschaften, Vereine, Religionsgemeinschaften, Parteien, Einzelhandel, Gaststätten – überall Windows und Office. Für die Nutzer ist das bequem: Sie stoßen in der Regel auf keine Schwierigkeiten, wenn sie beispielsweise ihre Steuererklärung abgeben wollen oder bei anderen Behörden Anträge einreichen wollen. In den Schulen lernen schon die Kleinsten den Umgang mit dieser Software. Die uniforme IT-Landschaft hat also nur Vorteile? Nein! Wenn man sich bei den Formaten der Daten, also bei Texten, Tabellen oder Präsentationen, auf ein freies, offenes Format einigen würde, wäre Vielfalt bei der Software möglich, ohne dass die Nutzer Nachteile hätten.

Entstanden ist aber eine Situation, in der Microsoft das Monopol bei den Formaten hat. Das ist problematisch, weil die Formate geschlossene Formate sind, bei denen man selbst mit großer Mühe und großem Aufwand nur teilweise klären kann, wie welche Daten gespeichert werden. Man muss davon ausgehen, dass in Texten, Tabellen oder Präsentationen Daten gespeichert sind, von denen der Nutzer nichts weiß, die aber für jeden, der Zugang zur Dokumentation der Formate hat, zu finden sind. Die Handelnden im tiefen Staat haben sicher Interesse an diesen Daten – und Zugang.

Ein Nebenaspekt ist, dass der Verfall von in diesen Formaten gespeicherten Daten vorprogrammiert ist, weil es nach gar nicht so langer Zeit nur noch mit großem Aufwand möglich sein wird, Programme zu finden, die diese Daten darstellen können. Versuchen Sie heute einmal, im Wordperfect-Format gespeicherte Dateien zu öffnen. Das war in den 90er Jahren das verwendete Standard-Dateiformat der Landesverwaltung in Nordrhein-Westfalen.

Geheime Software überall

Der eigentliche Skandal besteht aber darin, dass fast alle Software von Microsoft proprietäre Software ist, der Quellcode der Software also geheim ist. Anders als bei freier (Opensource) Software ist nur mit extrem hohem Aufwand herauszufinden, wie die Software arbeitet. Man kann deshalb nie sicher sein, ob die Software nur die von Microsoft behaupteten Funktionen ausführt. Genauso schwierig ist die Fehlersuche. Kriminelle nehmen diesen Aufwand in Kauf, weil er bei Erfolg Millionen-Gewinne verspricht; auch dadurch, dass gefundene Fehler nicht etwa schnellstmöglich behoben werden, sie werden vielmehr in einen Markt gegeben, auf dem auch Geheimdienste und andere staatliche Stellen einkaufen, um beispielsweise Schadsoftware („Trojaner“) auf den Rechnern der Nutzer zu platzieren und sie im Geheimen auszuspionieren. Die uniforme Ausstattung mit Software lädt dazu geradewegs ein.

> ***Insbesondere Organisationen mit kritischen Anliegen wie – ein Teil – der Parteien, Bürgerbewegungen, Aktionsbündnisse, … sind besonders bedroht. Sie sind auch bedroht, weil sie oftmals ihre Software nicht schnell genug aktualisieren und damit bekannte Sicherheitslücken lange Zeit bestehen bleiben und Angriffspunkte auch für Computer-Viren bilden.***

Welche Ausmaße die Angriffe durch Viren annehmen können, zeigte sich 2017, als der WannaCry-Virus (2) mehr als 230.000 Rechner lahmlegte. Betroffen waren unter anderem die Deutsche Bahn mit der Tochter Schenker, Krankenhäuser, Nissan und Renault, das US-Unternehmen FedEx, um nur wenige zu nennen. Selbstverständlich ist es nicht nur Kriminellen möglich, Rechner anzugreifen. Man kann davon ausgehen, dass dies auch staatlichen Stellen möglich ist, wenn beispielsweise eine Demonstrations-Vorbereitung gestört oder ein kritisches Magazin stillgelegt werden soll.

Dabei sind die staatlichen Stellen nicht auf den Einkauf von Sicherheitslücken angewiesen. Man muss davon ausgehen, dass sogenannte Backdoors, also geheime Zugangsmöglichkeiten, für sie in die Software eingebaut sind. Da die Software nicht überprüft werden kann, kann das nicht geklärt werden.

Aber warum im Geheimen die Nutzer ausforschen, es geht doch einfacher.

Es ist bekannt, dass die Möglichkeiten, die Nutzer auszuforschen, mit der aktuellen Version des Betriebssystems Windows 10 drastisch ausgeweitet wurden. Kein Wunder, dass Microsoft das Update auf diese Version kostenfrei angeboten hat, bei neuen Rechnern ist Windows 10 in der Regel vorinstalliert. Bekannt ist auch, dass sich diese Möglichkeiten auch mit großem Aufwand nicht vollständig ausschalten lassen. Die abgegriffen Daten werden an Microsoft weitergeleitet. Welche Daten das sind, wohin sie weitergeleitet und wozu sie genutzt werden, ist für die Nutzer nicht zu durchschauen. Das verbirgt der tiefe IT-Staat.

Das Ausforschen wird durch die Verwendung von Daten-Diensten zusätzlich unterstützt. Die Nutzung von Google zur Suche von Inhalten liegt trotz vorhandener Alternativen nur wenig unter 100

Prozent, obwohl vielen bekannt ist, dass Google den Suchverlauf speichert. Wer hat Zugang dazu und kann sich bedanken? Das Tracking (4) wird ergänzt durch die Nutzung von Google Maps. Wo der Nutzer war und wo er hin will, kann vielfach schon früh erkannt werden. Google-Mail wird auch in kritischen Kreisen viel verwendet, obwohl bekannt ist, dass Google Zugang zu den Inhalten der E-Mails hat; und nicht nur Google. Die Aufzählung kann fortgesetzt werden, das Ergebnis ist immer das Gleiche: Google erhält von den Nutzern umfangreichen Zugang auch zu sensiblen Daten.

Das tiefe IT-Netz der Geheimdienste

Dass auch die Geheimdienste ein tiefes IT-Netz betreiben, ist spätestens seit den Enthüllungen von Edward Snowden bekannt. Die Geheimdienste nutzen umfassend die beschriebenen Netze, ergänzt durch weitere Maßnahmen. Es ist bekannt, dass an den Knotenpunkten des Internets, in denen massenhaft Daten umgeschlagen werden, gezielt Abhörmöglichkeiten eingebaut wurden. Der Umfang der erfassten Daten übersteigt jede Vorstellungskraft. Die Geheimdienste verfügen inzwischen über die Möglichkeiten, die Daten ganzer Staaten in Echtzeit zu erfassen und zeitnah auszuwerten oder für die Auswertung vorzuhalten.

Alles nicht so schlimm?

Diesen Eindruck kann man gewinnen, wenn man die Reaktion der meisten Mitbürger sieht. Sie sind durch die Beschaffung und Nutzung von IT-Technik aktiv am Aufbau der Netze des tiefen IT-Staats beteiligt. Ein Smartphone muss wohl jeder haben, es daheim zu lassen oder es überwiegend auszuschalten geht nicht. Das wäre, nebenbei gesagt, auch kein kompletter Schutz gegen Überwachung,

da müsste schon der Akku entfernt werden. Auf den smarten Überwachungslautsprecher verzichten, wie uncool. Selbst das Wissen um die vertiefte Ausforschung und Überwachung lässt die meisten Leute kalt. Sogenannte soziale Netzwerke, die umfassend Daten sammeln, haben teilweise Milliarden von freiwilligen Nutzern.

Umfassende Aufklärung ist nötig

Es müsste also intensiv aufgeklärt werden. Nur durch wen? Das Schlimme ist, dass auch die Linken, die diese Aufgabe wahrnehmen müssten, sich ganz überwiegend nicht anders verhalten: Die Praxis unterscheidet sich trotz der direkten Bedrohung durch den tiefen IT-Staat kaum von der der „normalen“ Bürger. Anonym surfen mit Tor? Da erreiche ich ja nicht alle Seiten wie gewohnt. Facebook oder Instagram in Richtung freier Systeme verlassen oder sie wenigstens parallel betreiben? Das ist so aufwendig. Zudem leidet da doch meine Reichweite. Da empöre ich mich lieber ohne zu handeln. E-Mail-Verschlüsselung? Das soll doch so aufwändig sein. Außerdem habe ich keine Verschlüsselungspartner. Umstieg auf freie Software? Alle anderen nutzen doch auch das (Ausforschungs-)Betriebssystem Windows 10.

Die Linke muss endlich beginnen, sich mit dem tiefen IT-Staat und den Folgen der Digitalisierung ernsthaft auseinanderzusetzen. Sonst wird irgendwann der Stecker gezogen und dann ist das Klagen groß.

Was tun?

Da es sich bei dem IT-Staat um einen tiefen Staat handelt, ist es nicht möglich, sich ihm vollständig zu entziehen. Wer sich in der Öffentlichkeit bewegt, wird auf Überwachungskameras stoßen, denen er nicht entgehen kann. Wenn Sie zum Arzt gehen, den

Steuerberater aufsuchen, zum Psychiater gehen oder sich bei einer kirchlichen Stelle Rat suchen, immer müssen sie davon ausgehen das Daten zu Stellen gelangen können, wo sie nicht hingehören. Wer die Daten wann gegen die Bürger nutzt, ist unklar und nicht nachzuvollziehen. Ein tiefer Staat eben.

Das Wichtigste was getan werden kann, ist, dass Alle, die nicht zufrieden mit dem Zustand in diesem Land sind, endlich erkennen, dass sie durch den tiefen IT-Staat bedroht sind und sensibel dafür werden. Wenn man sich beispielsweise in politischen Zusammenhängen trifft, muss dafür gesorgt werden, das auf dem Hinweg, beim Treffen selbst und auf dem Rückweg keine Geräte, die Personen tracken, eingeschaltet sind und in der Wohnung alle Spionage-Geräte ausgeschaltet sind. Notfalls wird das Treffen ins Freie verlegt.

Notwendig ist, auch diesen tiefen Staat vertieft zu untersuchen und die Ergebnisse möglichst weit zu verbreiten. Bisher ist er ein blinder Fleck bei kritischen Menschen wie fast die gesamte IT-Technik. Das muss sich ändern. Bei Wahlen muss die Haltung der Parteien und ihre Praxis überprüft werden. Wo man kann, muss Einfluss genommen oder aufgeklärt werden. Muss mein Sportverein wirklich Windows und MS-Office verwenden?

Man kann sich aber auch als Einzelner zur Wehr setzen: Man entsorgt alle Geräte, die nicht zwingend ans Internet angebunden sein müssen: In den Kühlschrank schaut man wieder selbst rein, die Heizung wird wieder durch einfache Thermostate geregelt, man zieht sich einen Pullover an, wenn es zunächst zu kalt ist, wenn man nach hause kommt. Statt die Vorschläge des smarten Fernsehers zu akzeptieren, schaut man wieder in die Programmzeitschrift, eine vorhandene Kamera wird überklebt, wenn man sie nicht sicher Abschalten kann. Selbstverständlich werden alle vorhandenen Spionage-Lautsprecher entfernt.

Der Umstieg auf freie Software muss voran getrieben werden, bis man in der Lage ist, ein Betriebssystem zu nutzen, dessen Quellcode einsehbar und damit kontrollierbar ist. Beim Browsen schützt man sich gegen Tracking und andere Formen der Überwachung durch Ergänzungen (sogenannte Add-Ons) oder anonymes Surfen.

> ***Das Wichtigste aber ist: das Smartphone bleibt so oft wie möglich aus oder daheim, wenn nötig wird der Akku entfernt. Überwachungs-Netze wie Facebook, Instagram und Twitter werden verlassen, statt WhatsUp wird wieder SMS genutzt.***

Wird man so aktiv, werden die Daten, die zu einer Person gesammelt werden, drastisch verringert und insbesondere viele sensible Daten entstehen gar nicht erst. Die Überwachungs- und Aktionsmöglichkeiten im tiefen IT-Staat Handelnden werden erkennbar behindert. Wenn viele Bürger sich so verhalten oder wenigstens beispielsweise die Kirchen entsprechend handeln oder die Macher kritischer Webseiten Ausforschungsmöglichkeiten behindern, kann man hoffen, dass der Ausforschungs- und Überwachungsstaat an seine Grenzen stößt. Lasst es uns versuchen.

Anmerkungen und Quellen:

(1) Maurits Martijm + Dimitri Tokmetzis: Je hebt wél iets te verbergen, de Correspondent, 2016

(2) **https://www.googlewatchblog.de/2018/07/oeffi-google-oepnv-app/** (https://www.googlewatchblog.de/2018/07/oeffi-google-oepnv-app/)

(3) **https://de.wikipedia.org/wiki/WannaCry** (https://de.wikipedia.org/wiki/WannaCry)

(4) **https://www.eff.org/deeplinks/2018/10/privacy-badger-now-fights-more-sneaky-google-tracking**

(https://www.eff.org/deeplinks/2018/10/privacy-badger-now-fights-more-sneaky-google-tracking)

Wolfgang Romey arbeitete nach dem Studium der Theoretischen Elektrotechnik als Lehrer für Mathematik, Elektrotechnik und Digitaltechnik im Berufsbildenden Bereich, später als Lehrerausbilder im Vorbereitungsdienst, dem Referendariat. Dann folgte ein Wechsel in die Bezirksregierung Düsseldorf als Dezernent für Lehrerausbildung und später auch -fortbildung. Er verfügt über etwa 20 Jahre Erfahrung darin, angehende Lehrerinnen und Lehrer auf die Bildungsarbeit mit Digitalen Medien vorzubereiten und deren Urteilskraft in diesem Feld zur Entfaltung zu verhelfen. Die kritische Auseinandersetzung mit den dramatischen Folgen der Digitaltechnik, die ihm extrem unterentwickelt scheint, ist bis heute sein Thema.