Seit Snowden wissen wir: Überwachung ist immer und überall. Doch was ist technisch möglich, wird wirklich gemacht? Und sind „die USA“ wirklich „die Bösen“ und Deutschland einzig Opfer in diesem Spiel? Sind sichere E-Mail-Anbieter wirklich sicher? Und was kann jeder von uns im globalen „Informationskrieg der Geheimdienste“ zum Schutz der Privatsphäre und ob all der Desinformation eigentlich selber tun? Zu diesen Fragen sprach **Jens Wernicke** mit dem Hacker und Datenschutzaktivisten **Felix von Leitner**, der dank seiner kritischen Anmerkungen zu Politik und Zeitgeist als „Fefe“ inzwischen zu einem von Deutschlands meistgelesenen Bloggern avanciert ist, und gemeinsam mit Chaos-Computer-Club-Urgestein Frank Rieger den Podcast „Alternativlos“ herausgibt.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

http://www.nachdenkseiten.de/upload/podcast/160920_Die_Schutzmechanismen_haben_versagt_NDS.mp3

Podcast: Play in new window | Download

Herr von Leitner, Windows 10 spioniert uns aus, Android sowieso, Google weiß nahezu jedes Detail von uns und nun überwachen auch noch Fernsehgeräte unsere Wohnzimmer – nähern wir uns der total privat- sowie geheimdienstüberwachten Welt?

Ein Informations-Vorsprung ist schon immer ein Machtinstrument der Eliten gegen das Fußvolk. Auch moderne Demokratien pflegen oft das Selbstbild, dass das Volk im Wesentlichen zu desinteressiert oder uninformiert ist, als dass man sie an wichtigen Entscheidungsprozessen teilnehmen lassen darf. So wird gerne die repräsentative Demokratie als Staatsform legitimiert.

Wenn man sich innerhalb dieses Weltbildes bewegt, stellt sich fast automatisch das Bedürfnis ein, einen Informationsvorsprung gegenüber den normalen Bürgern aufrechtzuerhalten. Das ist Teil des Selbstbildes und damit Basis des Selbstwertgefühls. Wer keinen Informationsvorsprung aufbaut, muss wohl selbst Teil des Pöbels sein.

In früheren Zeiten gab es allerdings natürliche Grenzen dafür, wieviel Aufwand ein Überwachungsstaat treiben konnte. Sowohl das Einsammeln als auch die Auswertung der

Daten ist mit Aufwand verbunden. Wenn der Staat pro Verwaltungs-Fachkraft 10 Bürger überwachen kann, dann bräuchte man in einem Land wie Deutschland 8 Millionen Fachkräfte – tatsächlich beschäftigt die öffentliche Hand ungefähr die Hälfte, und die sind alle mit anderen Dingen ausgelastet. Und jetzt überlegen Sie mal, wenn jemand alle Ihre Äußerungen hören oder lesen und dann transkribieren, auswerten und in irgendwelche Aktenvermerke umsetzen müsste, dann erscheint der Faktor 10:1 sehr optimistisch geschätzt.

Erst die moderne Computertechnik ermöglicht es, praktisch ohne menschlichen Aufwand alle Kommunikationsdaten zu erheben und zu speichern. Die Auswertung ist zwar immer noch mit manuellem Aufwand verbunden – daran ist ja am Ende das System Stasi gescheitert; die kamen mit der Auswertung nicht hinterher. Aber auch hier gibt es „Hoffnung“ in Form von Experimenten mit künstlicher Intelligenz, Diktatsoftware ist beispielsweise inzwischen praktisch gut genug für den Produktiveinsatz beim Privatbürger. Google demonstriert, dass die Suche in Volltext-Daten ein gelöstes Problem ist.

Wir haben jetzt also alle Bausteine für einen perfekten Überwachungsstaat beisammen.

Für das Verständnis ist es wichtig, dass der Überwachungsstaat gar nicht perfekt sein muss, um eine Demokratie zu zerstören. Die Vermutung, überwacht zu werden, oder auch nur *möglicherweise* überwacht zu werden, führt bereits zu den gewünschten Verhaltensänderungen beim Bürger.

Und arbeiten private Unternehmen und Geheimdienste hier Hand in Hand, zwingen die Dienste die Unternehmen zur Kooperation – oder vertreten diese Kreise ohnehin Ihrer Meinung nach dieselben, weil elitären Interessen?

Das ist kein homogenes Feld. Einerseits gibt es Firmen wie AT&T, die schon seit Telegraphen-Zeiten freiwillig alle Daten an den Staat weitergeleitet haben, die der Staat gerne haben wollte. Seit ein paar Jahren wissen wir durch einen Whistleblower, dass das auch in Internet-Zeiten weiterhin so geblieben ist. Das Google-Stichwort ist „Room 641A“.

Andererseits gibt es Firmen wie Google, die sich wehren. Google hat in seinen internen Netzen starke Verschlüsselung angeschaltet, als sie gemerkt haben, dass die alle vom Staat angezapft werden. Aber inwieweit sich Firmen wehren können, hängt von der Gesetzeslage im jeweiligen Land ab. Und die ist gerade in den USA sehr unvorteilhaft. Aus weiten Teilen der Abhör-Gesetze wurde der Richtervorbehalt ganz getilgt – Stichwort „National Security Letters“ – und wo er noch nötig ist, wird er nicht offen, sondern verdeckt in einem Geheimgericht erwirkt – Stichworte „FISA Court“ oder „FISC“. Und Teil der staatlichen

Abhörersuchen ist regelmäßig auch eine Schweigeverpflichtung für die betroffene Firma.

Twitter prozessiert seit Jahren heroisch gegen die US-Behörden, um wenigstens Jahre später ihren Benutzern mitteilen zu dürfen, dass da mal Daten herausgegeben werden mussten. In einem Fall aus dem Wikileaks-Dunstkreis betraf das Birgitta Jónsdóttir, eine Parlamentsabgeordnete aus Island, bei der man jetzt als naiver Europäer nicht direkt angenommen hätte, dass sie unter US-Jurisdiktion fallen würde.

Hinzu kommt, dass wir inzwischen wissen, dass die Dienste sich im Inland tarnen. Die NSA macht ihre Zugriffe im Inland per Diensthilfeersuchen an das FBI. Für Google sieht das dann so aus, als würde das FBI eine ganz normale Anfrage im Rahmen einer strafrechtlichen Ermittlung machen.

Aber auch in Deutschland wird der Rechtsweg erschütternd häufig schon dadurch ausgeschlossen, dass dem Abgehörten gar nicht mitgeteilt wird, dass er gerade Opfer einer staatlichen Schnüffelattacke wurde. Was ich nicht weiß, dagegen kann ich mich auch nicht wehren.

Die Zuständigkeit legen sich die Behörden dabei gerne selbst sehr großzügig aus. So fand die US-Regierung, dass Microsoft E-Mails ihrer europäischen Bürger an die US-Behörden herausrücken muss, selbst wenn die Daten auf europäischen Servern in Irland liegen, nur, weil Microsoft selbst eine Firma mit Sitz in den USA ist. Dagegen konnte Microsoft sich in einem jahrelangen Rechtsstreit am Ende erfolgreich wehren. Aber alleine, dass diese Gerichtsverfahren überhaupt geführt werden mussten, lässt an der Stelle schon tief blicken.

Worin liegen aktuell die größten Gefahren für Privatsphäre und Datenschutz? Gibt es eine „neue Qualität“?

Nicht nur die technischen Überwachungsmöglichkeiten haben sich massiv zum Vorteil der Eliten und zum Nachteil der Bevölkerung entwickelt. Bei alltäglichen Handlungen fallen auch Größenordnungen mehr Daten als früher an. Wenn man vor 40 Jahren Geld abhob und im Supermarkt Lebensmittel einkaufte, dann fielen dabei nur beim Geldabheben am Bankschalter Daten an. Die Bank wusste natürlich, wer da Geld abhebt, weil man dafür eine Unterschrift leisten musste. Im Supermarkt zahlte man bar und im öffentlichen Nahverkehr prüfte nur der Busfahrer das Ticket, keine Maschine, die sich gleich noch die Seriennummer notiert.

Heute hat man in Form des Mobiltelefons die ganze Zeit einen Peilsender in der Tasche und man zahlt mit Karte. Jeder Dienstleister auf dem Weg kann wissen, wer ich bin. Die

Busgesellschaft, der Supermarkt, dazu kommt noch flächendeckende Kameraüberwachung und die Polizei hat sich mehrfach bei der „Funkzellenabfrage“ erwischen lassen, einer Art Rasterfahndung über die Positionsdaten der Mobiltelefone. Auf dem Weg nehmen wir vielleicht noch ein Selfie auf, in das die Kamera gleich die GPS-Koordinaten und die Uhrzeit einträgt, das laden wir dann zu Facebook, Instagram oder Twitter hoch, die damit auch informiert sind, wann wir wo waren.

In Kombination ergibt das eine nie dagewesene Bedrohung für unsere Privatsphäre, wenn man überhaupt noch davon sprechen kann, dass wir eine Privatsphäre haben. Wer von uns ist denn nennenswert lang täglich an einem unbekannten Ort, an dem keine Daten anfallen und wo er nicht beobachtet werden kann? Selbst ehemals überwachungsfreie Orte wie Fitnessstudio, Schwimmbad und Sauna sind inzwischen als Datenquelle erschlossen, weil die Leute Fitnesstracker und Smart Watches einsetzen. Nicht einmal im Zug oder einem Flugzeug über dem Atlantik ist man heutzutage mehr ohne Netzanschluss.

Diese Art von Überwachungsstaat kann man gar nicht ohne aktive, begeisterte Mitarbeit der Überwachten schaffen. Dafür war eine jahrelange Überredungskampagne nötig. Und jetzt glauben die Leute wirklich, dass sie unter dem Strich einen guten Deal machen, wenn sie alle ihre persönlichen Daten weggeben und dafür kostenlos im Internet an interaktiver Werbung teilnehmen dürfen.

Welche technischen Spionage- und Überwachungsdinge sind denn aktuell en vogue, den Menschen aber kaum bekannt? Was geht und wird bereits – ohne Wissen der Mehrheit – praktiziert?

Das ist gar nicht so leicht zu beantworten, weil der Staat sich beim Datensammeln ungerne in die Karten gucken lässt. Die Erfahrung zeigt, dass wenn etwas technisch möglich ist, dann wird es auch gemacht. Vielleicht nicht ab dem ersten Tag, ab dem es möglich ist, aber früher oder später wird es gemacht.

Dank der Arbeit von Professor Foschepoth wissen wir heute, dass die gesamte Existenz der Bundesrepublik Deutschland von Überwachung geprägt war. Das Grundgesetz hat es untersagt, also hat man mit den Siegermächten einen Deal gemacht, um gemeinsam eine Massenüberwachung aufrechtzuerhalten.

Die wichtigste Neuerung der letzten Jahre ist, dass Snowden bestätigt hat, dass die Überwacher unsere Kryptographie nicht brechen können und daher das System selber angreifen. Das funktioniert beispielsweise so, dass sie online bestellte Hardware bei der Zustellung abfangen, Hintertüren einbauen und dann das Gerät inklusive Hintertüren

zustellen.

Regierungen haben auf der Suche nach Hintertüren auch einen Schwarzmarkt für Wissen über Sicherheitslücken in Softwareprodukten geschaffen, die sie dann vor dem Hersteller verheimlichen, damit der sie nicht schließen kann. Die Angreifbarkeit unser aller Infrastruktur wird billigend in Kauf genommen, weil ein Hackangriff auf unsere Infrastruktur aller Wahrscheinlichkeit nach auch zu einer Budgeterhöhung für die Militärs und Geheimdienste führen würde.

Die Interessen der Bevölkerung spielen keine Rolle in diesem Kalkül. Die Dienste nehmen sogar in Kauf, dass sie selber über solche Sicherheitslücken angegriffen werden können, weil gegenüber dem Budget alle anderen Erwägungen zurücktreten. Die Aufgabe des militärisch-industriellen Komplexes ist in erster Linie der Machterhalt.

Vor kurzem hat zum Beispiel eine Gruppe namens „Shadow Brokers“ eine Sammlung an Exploits der NSA veröffentlicht, das sind Codeschnipsel, die jeweils spezifische Sicherheitslücken ausnutzen, deren Details die NSA auf dem Schwarzmarkt gekauft hat und dann geheim hielt. Mit diesem Herrschaftswissen kann die NSA dann den Rest der Welt angreifen.

Wer in seinem Privatleben jede unnötige Datenweitergabe und bekannte Angriffsmöglichkeit für Geheimdienste verhindern will, kann heutzutage kein selbstbestimmtes Leben mehr führen: Kein Uber, kein Smartphone, keine Kartenzahlung, kein „Internet of Things“; keine per App fernsteuerbaren Kühlschränke, Klimaanlagen, Feuermelder oder Stromzähler, keine Smart Watch, kein Bluetooth, kein WLAN, kein GPRS, kein UMTS. Tastatur und Maus mit Kabel, nicht mit Funk. Nur Dienste verwenden, die man selber betreibt. Alles mit Cloud bleibt außen vor. E-Mail nur auf dem eigenen Server, soziale Netze gehen nicht. Und dann stellt man fest, dass man sich aus weiten Teilen der Gesellschaft ausgeschlossen hat, weil man mit seinen Freunden auf Snapchat nur kommunizieren kann, wenn man auch auf Snapchat ist.

Ein solches Leben wird zunehmend unrealistisch und fühlt sich auch nicht wie ein selbstbestimmtes Leben, sondern nach einsamen Eremiten im Wald an, so jemandem wie Unabomber. So weit hat sich das Wertegerüst unserer Gesellschaft schon verschoben: Wer an der „freiwilligen“ Selbstentblößung nicht teilnehmen will, wirkt wie ein Aluhutträger, der auch daran glaubt, dass die Queen ein außerirdisches Reptil ist.

Gibt es für derlei „Hintertüren“ konkrete Beispiele oder zumindest begründete Vermutungen? Wenn ich Ihren Blog richtig verfolgt habe, vermutet man derlei

Hintertüren inzwischen in der Hardware von allen möglichen Herstellern? Bei YouTube gibt es etwa ein sehr aufschlussreiches Video von Peter Laackmann zu „Hardware-Trojanern in Security-Chips“, etwas, von dem „normale Menschen“ wahrscheinlich noch nie gehört haben bisher…

Der Nachweis von sowas ist immer sehr schwierig. Das schärfste Schwert für den Realitätsabgleich ist die eingangs genannte Maxime: Was möglich ist, wird auch gemacht. Und die Forschung hat in den letzten Jahren geradezu furchteinflößende Möglichkeiten gefunden. So gab es zum Beispiel eine wissenschaftliche Arbeit, die herausgefunden hat, dass man über die Dotierung des Siliziums im Wafer in der Chip-Fertigung verdeckt beispielsweise den Zufallszahlengenerator angreifen kann. Wenn der Zufall aber *nicht* zufällig ist, sind alle mit dieser Hardware durchgeführten Verschlüsselungsoperationen brechbar.

Wird das jetzt von den Diensten gemacht? Es ist kein Fall nachgewiesen, aber man muss wohl davon ausgehen, dass sie daran arbeiten.

Der für das Grundverständnis wichtige Teil ist, dass der, der die Hardware kontrolliert, alles damit machen kann. Wenn man sich ein Hintertür-Szenario denken kann, kann man das auch machen. Rein fundamentalistisch betrachtet haben wir daher bereits verloren, weil die Chips alle in Asien gefertigt werden. Wenn die uns Hintertüren installieren wollten, könnten wir da nichts gegen tun. Es war für mich daher ganz unterhaltsam, in den letzten Jahren die zunehmende Panik in der internationalen Cyberwar-Community zu beobachten, als diese Erkenntnis die Runde machte.

Und selbst, wenn wir die Prozessoren wieder selber fertigen würden, wären da immer noch die Mainboards, die Festplatten und SSDs, die Netzwerkkarten, die Sicherheitschips, die Netzteile, die Akkus, die Displays, die Tastaturen, die Mäuse. Das einzige echte Problem bei Wanzen in der Praxis ist, wie man die Stromversorgung garantiert. Alle Komponenten im PC mit Stromanschluss können also prinzipiell zu einer Wanze umgebaut werden, die Dinge rausfunkt, auf die sie Zugriff hat.

Für die Verteidigungsstrategie gegen sowas geht man davon aus, dass das prinzipiell möglich ist, aber dass nicht alle PC-Komponenten immer nach Hause funken, denn das Funkspektrum ist endlich. Da müsste also die konkrete Komponente, die ich hier gerade einsetze, speziell manipuliert sein. Dafür müssten die aber wissen, dass ich genau diese Komponente einsetzen werde, wenn sie mich angreifen wollten. Die Gegenwehr ist daher, dass man seine Komponenten nicht online kauft, sondern persönlich in einem Laden, bei dem man physisch vorbeifährt. Und hofft, dass unser Einzelhandel nicht schon in der Breite

kompromittiert ist.

Die Grenze zwischen ernsthaften Abwehrbemühungen und krasser Paranoia ist hier leider sehr fließend.

Peter Laackmann und Marcus Janke: „Spione an deiner Hintertür: Eine Reise auf die dunkle Seite der Macht“

Und der Silberstreif am Horizont? Die Hoffnung, dagegen vorgehen zu könne, meine ich…

Wenn wir diesen Trend nicht umgekehrt kriegen, gibt es nicht viel Hoffnung auf Besserung.

Solange sollte aber jeder für sich daran arbeiten, möglichst viele der obigen Empfehlungen umzusetzen. Man muss jetzt seine Hardware nicht barzahlend im Trenchcoat beim örtlichen Computerladen kaufen, weil man die Geheimdienste ärgern will. Aber Barzahlen ärgert auch die Datensammler aus den Werbeabteilungen und die örtlichen Händler zu bevorzugen, stärkt die lokale Wirtschaft und sichert Arbeitsplätze.

Und nicht bei den sozialen Netzen mitzumachen, hat auch andere Vorteile neben der Datensparsamkeit. Google muss meinen Terminkalender nicht kennen. Irgendwelche Webseiten müssen meine Telefonnummer nicht kennen. Wer mein Geburtsdatum oder meine Telefonnummer haben will, bei dem kaufe ich nicht. Webseiten, bei den man ohne Not einen Account einrichten soll, haben mich als User verloren.

Probieren Sie mal aus, wie gut es sich anfühlt, mal eine Entscheidung bezüglich der eigenen Daten *selber* zu treffen!

Zum Verständnis eine Nachfrage: Verstehe ich recht, dass Sie meinen, unsere Regierung nutze das Besatzungsrecht um, sozusagen über Bande und jenseits des Grundgesetzes, die eigene Bevölkerung massenüberwachen zu können? Sie glauben also nicht an die Geschichte vom „bösen Amerikaner“, der an allem schuld ist und das Böse in die Welt bringt; ich meine, ohne dessen Zutun Deutschland aus ausschließlich blühenden Landschaften ohne Unterdrückung und

Massenüberwachung bestünde? Auf Ihrem Blog nahmen Sie diesbezüglich ja etwa gerade De Maiziere ins Visier.

Ich glaube grundsätzlich nicht an Geschichten, die mit „der böse XYZ“ anfangen. Niemand tut Dinge, weil er böse ist. Alle halten sich für die Guten, wir haben nur alle unterschiedliche Wertesysteme und Weltbilder und gewichten die Freiheiten und Grundrechte anders.

Die Amerikaner hatten nach dem Krieg legitime Interessen, die sie durchsetzen wollten. Sie konnten sehen, dass die neue Bundesregierung nicht frei von Altnazis war – Google-Stichwort: „Hans Globke“ -, der Justizapparat war sogar recht flächendeckend problematisch. Da wollten die gerne das nächste Mal rechtzeitig informiert werden, wenn hier der Faschismus zurückkommt.

Überwachungs-Eingriffe sind immer eine Abwägung zwischen den Freiheitsrechten der Bürger und den Interessen des Staates, und aus Sicht der Amerikaner sind wir keine Bürger, sondern Ausländer. Daher fällt das Urteil dann für die Interessen des Staates aus. Da ist kein böser Wille dahinter.

Im Übrigen lief das Besatzerstatut 1989 aus und seitdem hört die Bundesregierung auch ohne Kooperation mit den Siegermächten ab. Wie das in der Praxis läuft, kann man in Bad Aibling sehen. Dort hat die NSA einen ECHELON-Stützpunkt betrieben und der wurde dann halt dem BND übertragen, der den Standort jetzt weiterbetreibt.

Ein Punkt, der mir ganz wichtig ist an der Stelle: Von der technischen Infrastruktur her ist das Abhören in Internet und anderen Netzen überhaupt kein Problem. Der Staat könnte sofort alles abhören, wenn er wollte. Man könnte schnell ein Gesetz machen oder wegen der akuten terroristischen Bedrohung den Notstand ausrufen und es einfach tun. Aber die sind nicht „die Bösen“, sondern die sehen sich als die Guten. Was ihnen nur noch fehlt, das ist eine moralische Legitimation, die auch vom Wahlvolk mit starker Mehrheit als legitim angesehen wird.

Auch unser Innenminister hat nicht das Ziel, einen Unterdrückungsstaat auszurufen. Aus dessen Sicht kann er seine Aufgabe, die Bevölkerung zu schützen, nur richtig wahrnehmen, wenn er uns alle vor uns selbst schützt. Aus diesem Blickwinkel wäre es auch akzeptabel, die Bevölkerung jeweils präventiv ins Gefängnis zu stecken, um sie vom Begehen von Straftaten abzuhalten. Aus Kostengründen würde man das nicht mit allen machen, sondern nur mit „Gefährdern“. Die entsprechende Rhetorik hat die Bundesregierung ja schon ausgerollt.

Die Einzelheiten sind allerdings historisch recht spannend – das Google-Stichwort lautet „G10-Gesetz“. Das G10 bezieht sich auf den Artikel 10 des Grundgesetzes, der das Fernmeldegeheimnis garantiert. Das G10-Gesetz regelt dann, wieso das im Einzelfall doch nicht gilt. Ich lade alle Leser ein, sich dieses Gesetz einmal aus der Perspektive durchzulesen, ob sie einen Fall konstruieren können, in dem dieses Gesetz gegen sie angewendet werden könnte.

Können Sie sagen, warum diese ganze Entwicklung offenbar immer rasanter und offenbar gefährlicher verläuft?

Die Kombination aus „die Leute geben uns freiwillig alle ihre Daten“ und „das Speichern von Daten wird immer billiger“ hat sehr viel Schaden angerichtet. Das Speichern von Daten ist so billig geworden, dass es inzwischen Standard in der Industrie ist, einfach *alle* anfallenden Daten zu speichern. Später wird sich schon etwas finden, was man damit machen kann. In vielen Fällen ist es auch tatsächlich so, dass noch keine Auswertung stattfindet und nur einfach alles gespeichert wird.

Die Preisentwicklung bei Massenspeichern ist sogar so, dass es regelmäßig billiger ist, einfach immer neue Festplatten nachzukaufen, und *nie* irgendwelche Daten zu löschen. Ohne Datenschutzgesetze gäbe es in der Praxis gar keinen Grund für Datenlöschung.

Der andere große Kostenfaktor bei der digitalen Datensammlung im Überwachungsstaat ist das Erheben der Daten. Dafür brauchte man früher teure Spezialhardware und der ständige technologische Fortschritt treibt den Preis beständig nach oben. Also haben sich die „Bedarfsträger“ – das ist die Bezeichnung für die Abhörer im Amtsdeutsch – vor ein paar Jahren mit dem Gesetzgeber abgesprochen, um diese Kosten auf die Netzbetreiber abzuschieben. Die Netzbetreiber haben jetzt bei der Anschaffung ihres Equipments darauf zu achten, dass es bereits eine Abhör-Hintertür eingebaut hat. Für diese Schnittstelle gibt es einen internationalen Standard. Wenn es sich nicht um Diktatur-Bedarf handeln würde, würde es rein äußerlich wie eine völlig normale, seriöse Sache wirken.

Man stelle sich mal vor, die Post verdoppelt das Porto, um damit die Miete und Gehälter für die Zentralstelle für Briefgeheimnisverletzung zu bezahlen! Früher war der Überwachungsstaat noch peinlich berührt von seinem Tun, ja, hatte sogar so etwas wie ein Unrechtsbewusstsein. Solche Eingriffe wurden daher aus undokumentierten schwarzen Budgets bezahlt, unter wunderschönen Tarnnamen wie „Bundesstelle für Fernmeldestatistik“. Man hat nicht am Ende noch das Opfer die Rechnung selbst zahlen lassen, wie in der berühmten Szene im Film „Brazil“.

Moment, da muss ich nachfragen: Jeder Internetprovider muss eine Hintertür für die deutschen Geheimdienste oder wen genau bereitstellen? Also auch all jene, die gerade – und seit Snowden – einen Massenandrang verzeichnen wie etwa Posteo oder Mailbox.org und bei denen die Menschen denken, sie wären der Überwachung nun ein für alle Mal entkommen? Die werden *alle* vollständig überwacht?

Das war die natürliche Reaktion des Staates auf die überwältigenden technischen Fortschritte. Früher war das so, dass der Privatsektor halt neue Methoden zum Datenverkehr über Satelliten erfunden hat und dann hat die NSA Möglichkeiten erfunden, an die Daten ranzukommen. Das lief einerseits über zusätzliche Bodenstationen im Sendebereich der Satelliten, andererseits über „Auffang-Satelliten“ im All hinter den tatsächlichen Satelliten. Unterseekabel hat man per U-Boot angezapft oder am Kabelende auf dem Land alles abgegriffen. Viele dieser Kabel sind internationale Kooperationen aus staatlichen oder ex-staatlichen Telekommunikationsunternehmen. Da kann man dann davon ausgehen, dass alle Länder, deren Telcos am Projekt beteiligt sind, da auch einmal die Daten ausleiten.

Aber so schnell, wie die technische Entwicklung ging, konnten die Dienste nicht Schritt halten. Daher wurde in den 1980er Jahren die Entscheidung getroffen, dass man schlicht für neu entwickelte Kommunikationsmethoden eine Abhör-Hintertür gesetzlich vorschreibt. Der Euphemismus für diese Abhör-Hintertüren ist „lawful interception“. Die US-Verordnung dazu heißt CALEA, die hat später den anderen Ländern als Vorbild gedient. In Europa muss man nach ENFOPOL googeln, die deutsche Version heißt Telekommunikations-Überwachungsverordnung.

Es gibt da internationale Standards, die treibende Kraft unter den Normierungsgremien war das Europäische Institut für Telekommunikationsnormen, ETSI. Das wissen wir durch die hervorragende Recherchearbeit von Erich Möchel, der im Jahre 2001 Dossiers über diese Normierungsarbeit veröffentlicht hat. Die ersten betroffenen Netze waren die GSM-Netze für Mobiltelefone. Aber auch alle anderen Dienste sind selbstverständlich betroffen, von Skype über Voice over IP bei der Telekom bis hin zu E-Mail und zukünftigen Diensten. Anbieter *müssen* eine genormte Schnittstelle anbieten, über die die Polizei oder mittels dieser dann die Dienste automatisiert Daten abgreifen können und zwar ohne dass der betroffene Diensteanbieter sehen kann, wer da gerade abgehört wird. Das will man auch so haben, denn sonst könnte ja ein Terrorist einfach selber eine kleine Telco aufmachen und wüsste dann immer, wenn er abgehört wird.

Wenn alle Dienstebetreiber Hintertüren vorhalten müssen, wieso raten dann einige Nerds, einen eigenen Mailserver zu betreiben? Das liegt daran, dass das Gesetz für die teureren

Anforderungen, u.a. für diese Schnittstellen, eine Mindest-User-Anzahl von 10.000 vorsieht (siehe hierzu die wichtige redaktionelle Anmerkung[*]). Wer also weniger als 10.000 Benutzer hat, muss keine Abhörschnittstelle vorhalten. Auf richterlichen Beschluss hin bleibt man natürlich trotzdem auskunftspflichtig.

Ich möchte nochmal betonen, dass alle diese Sachen nicht böse gemeint sind. Da saßen besorgte, alte Männer in einem Raum und haben sich Gedanken gemacht, wie man in Zukunft Polizeiarbeit gewährleisten kann. Dass sie auch den Grundstein für einen Überwachungsstaat legen, erschien ihnen das kleinere Übel im Vergleich zu dem vielbeschworenen „rechtsfreien Raum“.

Und es gibt da noch ein Detail, das vielleicht ganz interessant ist. Große Firmen und Behörden setzen Telefon-Nebenstellenanlagen ein. Die Telekom schaltet denen dann einen ganzen Bereich aus Rufnummern und die Durchwahl-Zuordnung am Ende übernimmt die Telefonanlage im Haus. Seit vielen Jahren gibt es die Geschichte, dass Russland für Telefonanlagen ein paar Features vorschreibt, die man als Hersteller dann halt einbauen muss, wenn man im russischen Markt verkaufen will. Eines dieser Features ist, dass man eine Nebenstelle so anrufen kann, dass das Telefon nicht klingelt, sondern sofort rangeht und dann den Raumton verdeckt überträgt. Sozusagen ein „Wanzen-Modus“. Natürlich sollte das in Deutschland nicht aktivierbar sein, aber wenn das in der Software implementiert ist, dann kann man das anschalten. Zur Not spielt man halt vorher die Russland-Version der Software auf.

Wissen Sie, was mich an *meiner* Rolle hier in diesem Gespräch gerade stört? Wir Journalisten, die wir aufklären wollen über das, was geschieht – wir betreiben doch klammheimlich das Geschäft der Überwacher mit, wo wir immer nur auf die Totalität der Überwachung abstellen und damit Ohnmacht verbreiten. „Alles furchtbar!“ ist doch nicht, was Hoffnung verbreitet und Widerstand schürt.

Der Skandal ist aus meiner Sicht nicht, dass der Staat tut, was er tut. Sondern dass niemand von uns das verhindert hat. Die Öffentlichkeit hatte die Möglichkeit, sich zu informieren und etwas zu tun. Nicht über alle Details, aber über die grobe Richtung. Spätestens seit 2000 hätten alle wissen können, was die Geheimdienste machen und wie wenig moralische Grenzen es gibt. Da gab es einen Report von Duncan Campbell für das EU-Parlament über ECHELON, das globale Abhörsystem der Five Eyes. Der Bericht heißt „Interception Capabilities 2000“ und steht frei im Internet zum Download.

Es passierte damals, was heute wieder passiert nach Snowden: Die EU heuchelt Schock und Überraschung und alle Länder nehmen dann die Fähigkeiten der NSA intern als Maßstab

dafür, was „unser Geheimdienst auch können sollte“.

So gut wie niemand leistet tatsächlich Fundamentalopposition gegen Überwachung. Die PR-Spezialisten von Bertelsmann und Co. haben es geschafft, Datenschutz zu einer Art Schimpfwort zu machen: Jemand erwähnt Datenschutz, alle rollen mit den Augen. Datenschutz, das sind doch diese Leute, die immer nur Ärger machen und uns vom Arbeiten abhalten hier!

Das ist unsere Schuld. Wir können nicht auf die Regierung zeigen. Es gab mehr als genug Wahlen seitdem. Das Grundgesetz hätte uns vor diesen Diktatur-Vorläufern schützen sollen. Die Deklaration der Menschenrechte hätte uns schützen sollen. Wir reden immer von der wehrhaften Demokratie. Wieso hat diese uns nicht vor dem Überwachungsstaat geschützt? Wieso hat uns die Gewaltenteilung nicht geschützt? Die Presse?

Selbst wenn wir die ganzen Überwachungs-Geschichten jetzt zurückrollen, finde ich persönlich die viel schlimmere Nachricht, dass uns keiner unserer Schutzmechanismen geschützt hat. Was ist unsere Demokratie eigentlich wert, wenn sie sich einfach so unterminieren lässt?

Aber zu Ihrer Frage zurück: Ja, viele Menschen sehen angesichts der möglichen oder tatsächlichen Übermacht des Überwachungsstaates kaum mehr eine Möglichkeit der Gegenwehr. Argumente wie “wenn die mich überwachen wollen, können sie es eh tun, also kann ich auch meine Selfies bei Facebook hochladen” greifen aber zu kurz. Der Überwachungsstaat ist heute wie damals mit Aufwand und Kosten verbunden. Daten kopieren, die freizügig herausgegeben werden, kostet so gut wie nichts. Daten entschlüsseln oder gar Computer individuell aufhacken, weil man die Verschlüsselung nicht brechen kann, ist hingegen teuer und aufwendig. So teuer, dass es nicht in der Breite geht, sondern nur in Einzelfällen. Die einfachste und beste Verteidigung gegen den Überwachungsstaat ist daher, es den Überwachern so unangenehm und teuer wie möglich zu machen, indem man sich in Datensparsamkeit übt und alle Daten nur verschlüsselt abspeichert und überträgt.

Schritt 1: https:// statt http://, nicht nur beim Onlinebanking, sondern auch bei Google und sonst überall. Facebook per https ist immer noch unnötige Datenweitergabe, aber es ist nicht ganz so schlimm wie Facebook per http. Hier haben wir in den Jahren seit Snowden enorm Boden gutgemacht.

Schritt 2: Immer den Browser und das Betriebssystem aktuell halten. Am besten obsessiv jeden Morgen manuell den “Nach Updates suchen“-Knopf klicken.

Schritt 3: Gewohnheiten ändern. Daten nicht ohne Not weitergeben. Keine sozialen Netze mehr, keine Cloud-Dienste. Wo ein Totalausstieg sich nicht sofort umsetzen lässt, zumindest alle Datenschutzeinstellungen durchgehen und unnötige Datenweitergabe ausschalten. Der Browser etwa muss keine Statistiken an den Hersteller weitergeben. Und Adblocker im Browser sind, nicht nur aus Datenschutzgründen, sondern auch weil die Werbenetzwerke sich immer wieder für das Verbreiten von Schadsoftware missbrauchen lassen, digitaler Selbstschutz.

Schritt 4: Sich über Datenschutz- und Freiheitsaktivisten informieren und mal hingehen, mit den Leuten reden. Der größte Feind der Freiheitsrechte sind Leute, die nicht für ihre Rechte kämpfen, weil sie den Kampf schon verloren wähnen.

Auf Ihrem Blog kritisieren Sie seit einiger Zeit die Amadeu-Antonio-Stiftung, die auch auf den NachDenkSeiten bereits in der Kritik stand. Worum geht es dabei?

Die Amadeu-Antonio-Stiftung wird vom Bundesministerium für Familie, Senioren, Frauen und Jugend gefördert und tritt bei einer Kampagne gegen „Hate-Speech“ als Berater und Dienstleister des Ministeriums auf.

Ich habe oben skizziert, wie aus meiner Sicht alle Schutzmaßnahmen versagt haben, den Überwachungsstaat aufzuhalten. Aktuell gibt es nur noch zwei bestehende Barrikaden, die dem Überwachungsstaat im Weg stehen. Erstens, dass im Internet Menschen Webseiten wie die NachDenkSeiten aufmachen und lesen und dort weitgehend unbelästigt vom Staat ihre Meinung sagen und vor Entwicklungen warnen können. Und zweitens, dass Programmierer „Guerilla-Lösungen“ wie Verschlüsselung für E-Mail, Chat, Messaging, Telefonie, Videokonferenzen sowie Verschleierungslösungen wie Tor für anonymes Web-Klicken schaffen.

Unter dem Label der Bekämpfung von „Hate-Speech“ wird jetzt eine moralische Grundlage für das Unterdrücken von unerwünschten Meinungen im Internet geschaffen. Das sieht vielleicht für Außenstehende nicht nach einem Zensurversuch aus, aber für Nerds gibt es da eine Geschichte dahinter. Denn die Regierung versucht seit Jahren, eine moralische Relativierung für Internetzensur zu finden und hat es zuvor bereits mit Terrorismus und Kindesmissbrauch versucht.

Diese Versuche sind gescheitert. Der aktuelle Versuch mit Hate-Speech als Vorwand scheint hingegen zu funktionieren, zumindest bisher. Er wirkt auf mich wie der Versuch, die Zensur-Opposition gezielt und unter dem Vorwand der Terrorismusbekämpfung aufzuspalten.

Mal ganz zynisch gesprochen: SPD und CDU erzählen den Wählern auch seit Jahren, die SPD sei links und die CDU sei rechts und es gäbe da Unterschiede und die seien wichtig und die Menschen müssten sich zwischen links und rechts entscheiden und dann gegenseitig bekämpfen und verachten. Und jetzt probieren sie diese Masche bei den Nerds: „Es gibt Gut und Böse, zu bekämpfende und zu unterstützende Zensur“, lautet das Kredo dabei. Diesen faulen Versuch interpretiere ich als Ausdruck der Geringschätzung für Menschen wie uns.

Ich unterstelle der Stiftung da keinen bösen Willen. Ich glaube nicht, dass die verstanden haben, was sie da fordern und welche Auswirkungen das hat. Die werden nicht das Ziel haben, der Sargnagel für die Demokratie in Deutschland zu sein. Aber sie sind eben das öffentliche Gesicht dieser Kampagne und kriegen daher auch die ganze Kritik, den Ärger und die Empörung ab. Die Stiftungs-Reaktion wirkt auf mich dabei so, als ob die überhaupt nicht verstehen, was den Ärger ausgelöst hat und wieso die Leute alle zu ihnen kommen damit.

Etabliert wird also gerade eine … ja, „Zensurinfrastruktur“, zu deren moralischer Rechtfertigung eine sich selbst als links verortende Stiftung maßgeblich Anteil nimmt? Was meint das konkret?

Zensur funktioniert heute nicht mehr über eine Behörde, die bei Redaktionen Akten beschlagnahmt und Hausdurchsuchungen macht und Journalisten einlocht. Zensur funktioniert heute so, dass man bei Facebook einen Knopf klickt, und ein Callcenter in Irland löscht dann Inhalte. Bei der Behörde hat man wenigstens die Illusion eines Rechtswegs.

Zensurbestrebungen sind dabei generell unabhängig von der politischen und religiösen Orientierung. Zensur ist ein inhaltlich neutrales Machterhaltungsinstrument, das den Eliten dient, um den Rest der Bevölkerung daran zu hindern, sich darüber auszutauschen, was das Problem ist, dass es *überhaupt* ein Problem gibt und man nicht der Einzige ist, der sich das fragt und was hiergegen getan werden muss.

Das Problem ist auch, dass das Internet ein kooperatives Medium ist. Zensur ist im Internet keine Sache, die mit Gewaltausübung oder -androhung zu tun hat. Jede Maschine auf dem Weg zwischen mir und meinem Kommunikationspartner kann nicht nur sehen, was ich sage, sondern es auch manipulieren. Technisch kann ich mich dagegen nur wehren, indem ich starke Verschlüsselung verwende.

Der Staat möchte seit vielen Jahren erreichen, dass ich keine starke Verschlüsselung verwenden darf, die die „Bedarfsträger“ nicht entschlüsseln können. Das Stichwort für

diesen Konflikt heißt „Crypto Wars“.

Frankreich hat eine Weile schlicht starke Schlüssellängen verboten. Man durfte also verschlüsseln, aber nur mit schwacher Verschlüsselung, die die Geheimdienste brechen konnten. Russland hat Verschlüsselung gleich ganz verboten. China blockiert verschlüsselte Datenübertragung in ihrer Firewall. Die USA haben stattdessen vorgeschlagen, dass man verschlüsseln darf, aber den Schlüssel bei einer „vertrauenswürdigen Stelle“ hinterlegen muss, wo die Polizei und Geheimdienste „im Notfall“ rankommen. Als die USA damit scheiterten, haben sie sich auf „dann hacken wir halt eure Computer“ zurückgezogen.

Der Euphemismus dafür ist übrigens „Cyber“. Wenn Regierungen von Cyber reden, meinen sie sowas. Von „Abwehr“ und „Defense“ darf man sich an der Stelle nicht ins Bockshorn jagen lassen. Die Gelder im Cyberwar-Bereich gehen im Moment weltweit praktisch vollständig in offensive Praktiken.

„Zensurinfrastruktur“ ist an dieser Stelle ein Kampfbegriff. Es geht nicht wirklich um den *Aufbau* einer Infrastruktur, denn die ist längst da. Nerds sehen die Schranke hier auch viel geringer als untechnische Menschen. Das Stichwort ist Netzneutralität. Wenn man subtil manipulierte Inhalte auf Facebook sehr schnell ladend kriegt und anderswo langsam ladend, aber unmanipuliert, dann werden die Leute sich ihre Nachrichten bei Facebook holen. Das klingt nicht wie Zensur im traditionellen Wortsinn, aber man muss es in diesem Kontext betrachten.

Für eine Zensurinfrastruktur reicht es in diesem Sinne bereits aus, wenn Menschen sich nicht mehr trauen, bestimmte Themen zu diskutieren oder bestimmte Thesen zu diskutieren, weil sie mit einem öffentlichen Pranger rechnen müssen, wie ihn die Amadeu-Antonio-Stiftung nicht nur vorgeschlagen, sondern bereits betrieben hat. Der Pranger war nicht für Hate-Speech sondern für „Neue Rechte“, also ein anderes ihrer Projekte.

Freie Meinungsäußerung ist eine der Grundfesten der Demokratie, an der wir meiner Meinung nach nicht rütteln dürfen. Und insbesondere heißt freie Meinungsäußerung, dass unbeliebte Minderheiten auch unbeliebte Positionen vertreten dürfen. Denn die anderen dürfen eh ihre Positionen frei vertreten. In meinem politischen Weltbild muss eine Demokratie es aushalten, wenn Extremisten widerliche Positionen öffentlich vertreten. Niemand muss hingehen und sich das anhören, das Fernsehen muss das nicht übertragen. Aber äußern müssen sie es dürfen.

Die Amadeu-Antonio-Stiftung vertritt hingegen die Position, dass die Unterdrückung von Äußerungen okay ist, wenn sie nur als „Hate-Speech“ eingeordnet werden können. Das ist

eine politische Position, die man haben kann und ich finde es gut, dass sie die äußern dürfen. Aber ich muss dann dagegen opponieren. Denn das öffnet Tür und Tor für die Unterdrückung jeder unliebsamen Meinung, das ist alles nur eine Frage der entsprechenden Definition.

Quelle: AcTVism Munich

Am 19. Januar dieses Jahres gaben Sie bekannt, aus dem Chaos Computer Club Berlin ausgetreten zu sein. Warum dieser Schritt? Steht der CCC nicht für „digitalen Widerstand“?

Mein Austritt aus dem CCC bezog sich auf eine interne Debatte im CCC, bei der ich glaubte, ein Signal senden zu müssen, um die Mitglieder wachzurütteln.

Mit den Zielen des CCC fühle ich mich nach wie vor verbunden und im CCC kämpfen auch die richtigen Leute mit den richtigen Methoden die richtigen Kämpfe für die richtige Sache.

Diese Art von „Rette sich wer kann!“-Mentalität scheint aktuell ja um sich zu greifen – auch und gerade in linken Kreisen. Ärgert Sie das? Dass allerorten Moral und Anstand gepredigt werden, offenbar aber einer nach dem anderen die Seiten wechselt?

Eine der wichtigsten Einsichten im Leben ist meiner Meinung nach, dass wir alle irrational sind. Jeder hält sich selbst für den einzigen rationalen Denker hier und die anderen für Spinner. Aber im Allgemeinen handeln die Menschen innerhalb ihres Realitätsmodells rational. Mein Weltbild ist nicht besser als das von irgendjemand anderem. Die Handlungen anderer basieren bloß auf anderen Prämissen.

Die Leute lügen auch nicht, wenn sie Moral und Anstand predigen. Aus ihrer Sicht vertreten sie Anstand und Moral und arbeiten für das Gute. Möglicherweise gehen sie andere Kompromisse im Namen des guten Ziels, das sie erreichen wollen, ein.

Ich sehe ehrlich gesagt nicht, dass hier massenweise Leute die Seiten wechseln. Ich halte im Gegenteil diese Seiten-Ideologie für eines der Hauptprobleme unserer Zeit. Leute

legitimieren das Unterdrücken von inhaltlichen politischen Positionen damit, dass diese „von der anderen Seite“ käme. Bei den Linken ist es inzwischen wohl sogar üblich, Positionen zu unterdrücken, weil derjenige, der sie vorträgt, mal mit jemandem „von der anderen Seite“ zusammen gesehen wurde.

Selbst wenn man mal annimmt, dass es verschiedene Seiten gibt. Dann muss man sich doch gerade die Positionen der anderen Seite auch anhören, denn die der eigenen Seite kennt man ja schon! Die vertritt man ja selber! Welchen Erkenntnisgewinn kann es denn geben, wenn man sich nur die Argumente anhört, die man selber vertritt?

Ich persönlich finde das nicht schlimm, wenn jemand Anstand und Moral als Begründung bringt. Das ist mir lieber, als wenn jemand überhaupt keine Argumente bringt, weil er das eh alles für selbstverständlich hält oder weil es angeblich keine Alternativen mehr gibt.

Was braucht es zurzeit? Und: Was können wir als Einzelne tun?

Was wir brauchen, sind mehr Empathie und eine Rückkehr zum Solidargedanken, mehr Zusammenarbeit und weniger Kämpfen, mehr Respekt voreinander.

Und wir dürfen uns nicht mehr so billig unsere Privatsphäre und andere Freiheitsrechte abkaufen lassen.

Ich bedanke mich für das Gespräch.

Felix von Leitner, Jahrgang 1973, ist einer der meistgelesenen deutschen Blogger und unter dem Pseudonym Fefe bekannt. Er ist Geschäftsführer und Inhaber eines auf IT-Sicherheit spezialisierten Unternehmens. Von Leitner war lange Jahre Mitglied des Chaos Computer Clubs (CCC) Berlin. Gemeinsam mit CCC-Urgestein Frank Rieger veröffentlicht er den unregelmäßig erscheinenden politischen Podcast „Alternativlos“.

Weiterschauen:

Edward Snowden, Glenn Greenwald & Noam Chomsky: Unterhaltung über Privatsphäre, Teil 1

Edward Snowden, Glenn Greenwald & Noam Chomsky: Unterhaltung über Privatsphäre, Teil 2

Weitere Veröffentlichungen von **Jens Wernicke** finden Sie auf seiner Homepage jenswernicke.de. Dort können Sie auch **eine automatische E-Mail-Benachrichtigung** über neue Texte bestellen.

[«*] **Wir weisen in diesem Zusammenhang darauf hin, dass E-Mail-Provider dieser Aussage bereits öffentlich widersprochen haben. Sie etwa: „Posteo zur Mär von der ‚Abhör-Schnittstelle‘“. Konkret heißt es vonseiten etwa Posteo: „Die Computerzeitschrift c`t schreibt hierzu in Ihrer aktuellen Ausgabe (4/2014): “E-Mailprovider mit mehr als 10.000 Kunden müssen eine so genannte SINA-Box betreiben, die den Mailverkehr aller Kunden ausleiten kann, ohne dass es der Provider oder der Kunde bemerkt.” Das ist falsch.** Es ist deutschen Behörden nicht möglich, ohne das Wissen eines Providers auf E-Mails von Nutzern zuzugreifen. Und eine SINA-Box hat keinen Zugriff auf die Systeme eines Providers. **Wir haben die Redaktion um Richtigstellung gebeten. Sie hat den Fehler inzwischen eingeräumt und eine Richtigstellung im c’t-Blog veröffentlicht. Da wir nicht alle Anfragen persönlich beantworten können, möchten wir nun an dieser Stelle darüber informieren, wie es sich mit der SINA-Box verhält:** Bei Posteo steht bisher keine SINA-Box.“