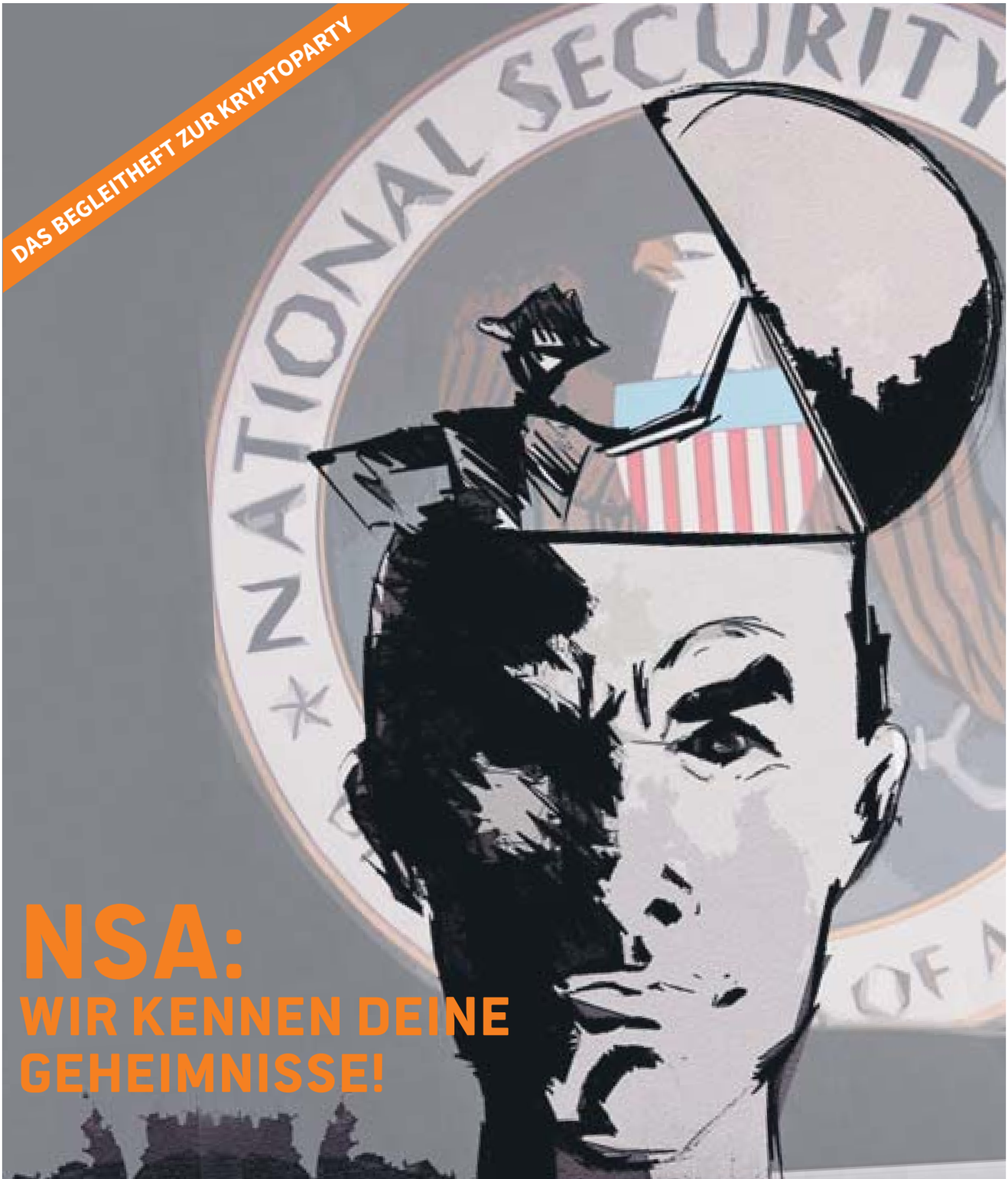
2013.NSA

KOMPASS

//kompass.im

Demokratie und Freiheit, Bürgerrechte und informationelle Selbstbestimmung, Transparenz in Politik und Staat, existenzielle Sicherheit und gesellschaftliche Teilhabe, freier Zugang zu Information und Bildung, ein bürgerfreundliches Urheber- und Patentrecht, sowie weitere Themen, die Piraten bewegen

DAS BEGLEITHEFT ZUR KRYPTOPARTY



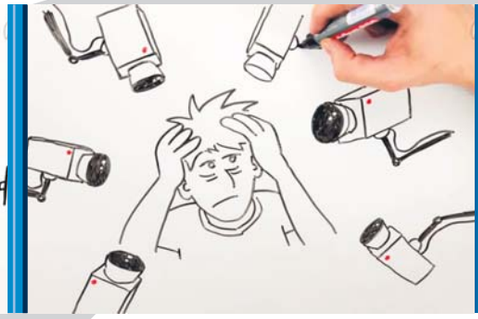
NSA:
WIR KENNEN DEINE GEHEIMNISSE!

illustration: CC BY-SA: be-him

FREIHEIT STATT ANGST UND ÜBERWACHUNG

BITTE RECHT FREUNDLICH

Überwachung Kameras vor dem Haus, angezapfte Handys und immer wieder diese Stimme im Hinterkopf – ein Bericht aus dem Alltag einer Observierten.



Ich weiß, wie es sich anfühlt, vor der eigenen Haustür zu stehen und eine Kamera im Rücken zu haben. Ich wusste nie genau, wo sie war, aber ich habe inzwischen die Protokolle der Aufzeichnungen gelesen. „Mann mit Kleinkind und leeren Getränkekisten verlässt das Haus." Eine halbe Stunde später: „Mann mit Kleinkind betritt das Haus", steht da zum Beispiel über meinen Freund und unsere Tochter. Ich habe auch die Kommentare zu meinen eigenen Telefonaten gelesen, die die Beamten mitgehört haben. Lange habe ich die Lektüre allerdings nicht ausgehalten. Mir wurde davon übel.

Ende Juli 2007 wurde Andrej Holm, mein Freund, morgens um sieben in unserer Wohnung festgenommen. Der Vorwurf lautete, er sei ein Terrorist, Kopf und Texteschreiber der „militanten gruppe (mg)", der Brandanschläge auf Autos und Gebäude zur Last gelegt werden. Andrej wurde im Hubschrauber nach Karlsruhe zum Bundesgerichtshof (BGH) geflogen, der Richter unterschrieb einen Haftbefehl und Andrej verschwand in Untersuchungshaft in Berlin-Moabit. Nach drei Wochen wurden dem Ermittlungsrichter die kritischen Medienberichte und Briefe zu viel und er verschonte Andrej von der Haft; zwei Monate später hob der BGH den Haftbefehl auf und erklärte, dass der nie hätte unterzeichnet werden dürfen. 2010 wurde das Verfahren eingestellt. Eines aber wirkt bis heute nach: Die Erfahrung, wie es ist, als Angehörige eines Terrorverdächtigen überwacht zu werden.

Wie wir inzwischen aus den Ermittlungsakten wissen, hat die Überwachung schon ein Jahr vor der Festnahme begonnen: Unsere Telefone, Handys und Büroanschlüsse wurden abgehört, Zivilbeamte observierten, lasen E-Mails mit und protokollierten das Surf-Verhalten im Internet, sie brachten GPS-Peilsender an Autos an, stellten Video-Kameras vor und hinter dem Haus auf und schossen heimlich Fotos auf der Straße.

Eine Woche nach der Entlassung wurde unsere Wohnung noch einmal durchsucht. Die Beamten hatten ein Telefonat mit Andrejs Mutter falsch interpretiert und glaubten allen Ernstes, in ihrer Wohnung wäre heißes Beweismaterial gelagert gewesen, das zum sonntäglichen Kaffeetrinken zu uns transportiert werden solle. Ergebnis: Auch Andrejs Eltern wurden observiert und sind nur um Haaresbreite selbst einer Durchsuchung entgangen. Wir alle waren noch nicht gewohnt, uns am Telefon auch für Dritte immer klar und deutlich auszudrücken, und so hatte Andrejs Mutter einen Satz formuliert, der nur für Andrej verständlich war: Mit dem „Inhalt des schwarzen Beutels" waren allerdings nicht etwa Brandsätze gemeint, sondern die aus dem Gefängnis nach Hause transportierten Ermittlungsakten.

DREH DICH NICHT UM, DAS HALTEN DIE FÜR VERDÄCHTIG

Anfangs schien mir die Überwachung nicht einmal das Schlimmste. Ich hatte eine 16 Stunden dauernde Hausdurchsuchung erlebt, hatte Kindern, Verwandten, Freunden und Kolleginnen erklären müssen, warum Andrej verschwunden war. Hinzu kam die Ungewissheit. Die Begründung der Staatsanwaltschaft für die Haft war absurd gewesen. Wenn so etwas möglich war, war auch eine Haftstrafe vorstellbar.

Irgendwann bemerkte ich eine Stimme in meinem Kopf: „Dreh dich auf der Straße nicht um! In den Akten stand, dass sie das bei Andrej verdächtig fanden." – „Mach keine Witze über Brandanschläge am Telefon! In den Akten stand, dass sie das in einem Telefongespräch mit deiner Mutter angestrichen haben." Dabei war ich selbst ja gar nicht verdächtig. Meine Telefonate wurden trotzdem abgehört und in den Akten kommentiert.

Menschen verhalten sich anders, wenn sie wissen, dass sie beobachtet werden. Wer für sich anderes behauptet, stelle sich morgens beim Aufstehen eine Kamera vor, die dies live ins Internet überträgt. Ich habe zwei Monate nach Andrejs Festnahme begonnen, über unseren Alltag mit der Überwachung zu bloggen. Ich blogge weiter, schreibe und rede über dieses und ähnliche Verfahren, über die Instrumentalisierung von Angst, über Terrorismus, über den scheinbaren Widerspruch von Freiheit und Sicherheit.

Und wenn ich über diese Themen schreibe, habe ich diese Stimme im Ohr. Vergangene Woche habe ich auf freitag.de den Text „Terror it is?"veröffentlicht, der sich damit beschäftigt, dass nach den jüngsten Brandanschlägen auf die Bahn in Berlin wieder von Terrorismus gesprochen wird. Und schon beim Schreiben, am Anfang eines Textes über Brandanschläge, höre ich die Stimme fragen, ob das klug ist. Immerhin haben sie Andrej das Schreiben von Texten vorgeworfen, nicht das Legen der Brände. Der Beginn der Ermittlungen war, so das Bundeskriminalamt, die Übereinstimmung von verdächtigen Wörtern in seinen Texten mit denen in Anschlagserklärungen.

Wenn ich diesen Text schreibe, dann lesen die das auch. Und sie nehmen einen Kommentar in die Akten, dass ich mich offenbar für Brandanschläge interessiere. Auch jetzt frage ich mich, ob es klug ist aufzuschreiben, dass ich mir darüber Gedanken mache, was die davon halten. Wäre es nicht besser und einfacher, über andere Themen zu schreiben? Es gibt ja genug. Ich verbiete mir,

Impressum
Herausgeber: Denk Selbst e.V. Verantwortlich im Sinne des Presserechts: Michael Balke. Mitarbeit: Jürgen Asbeck/Timecodex, Michael Balke, Radbert Grimmig, Stefan Müller, Anne Roth, Ulrich Scharfenort/ulrics. Dank an Der Freitag (http://www.freitag.de) für den Artikel von Anne Roth, manniac.de, Udo Vetter.

mich davon einschränken zu lassen, aber die Stimme ist da.

MUSST DU DENN AUSGERECHNET ÜBER BRANDANSCHLÄGE SCHREIBEN?

Der vom Chaos Computer Club entdeckte Staatstrojaner, das erste bekannte Beispiel einer möglichen Online-Durchsuchung, hat unter anderem deshalb so viel Aufmerksamkeit erregt, weil er über das Netz weitere Programme nachladen und ferngesteuert zur Ausführung bringen kann. Die verschiedenen zuständigen Innenpolitiker bemühen sich, dies zu einer Art Versehen herunterzuspielen, weil gewissermaßen nie eingeplant war, die Funktion zu nutzen.

Überwachung musste ausgeweitet werden. Dass ausgerechnet bei der Online-Durchsuchung das Muster „Wir finden nichts, also muss die Überwachung ausgeweitet werden“ nicht zum Einsatz käme, kommt mir zumindest wenig wahrscheinlich vor.

WENN DU DICH BEMÜHST, ETWAS ZU VERBERGEN, GUCKEN DIE NACH

„Ich habe nichts zu verbergen.“ Wenn in den vergangenen Jahren über Datenschutz, Überwachung, Google oder das Recht auf die Verwendung von Pseudonymen diskutiert wurde, ist kaum ein Satz häufiger gefallen als dieser. Manche Vertreter der Post-Privacy-Idee sagen: „Bemüht Euch nicht, irgendwas zu verbergen, demnächst

waltschaft eine Fluchtgefahr, weil die – für die Aufhebung der Untersuchungshaft nötige – enge familiäre Bindung ja offenbar nicht gegeben sei. Treffen mit Freunden wurden zu Kontaktaufnahmen mit weiteren Verdächtigen. Telefongespräche, bei denen es um einen geplanten Kneipenabend ging, wurden zu konspirativ verabredeten Treffen, weil Adresse, Zweck und Namen aller Beteiligten nicht explizit genannt worden waren. Aus einem vergessenen Handy wurde eine typisch linksextreme Verhaltensweise. Entlastende Interpretationen gab es nicht.Alle diese Beispiele dienten der Begründung, warum die Überwachung ausgeweitet werden musste, warum ein Haftbefehl nötig war, warum die Untersuchungshaft weiter nötig war.

Je nach Grad des Misstrauens in die Staatsmacht erfüllen uns die Versicherungen, dass das gar nicht so gemeint war, mit Zweifeln. Wenn die Möglichkeit des Hochladens von Erweiterungen auf den überwachten Rechner in der Software existiert, dann ja sicherlich nicht, weil sie nie genutzt werden sollte. Wann also sollte sie zum Einsatz kommen? Selbst wenn wir mal die Petitesse beiseite lassen, dass schon allein die technische Möglichkeit vom Verfassungsgericht als Verstoß gegen das Grundgesetz gewertet wird, ist davon auszugehen, dass erst die abgespeckte Version des Trojaners zum Einsatz kommen sollte und später – so sich der Verdacht erhärtet – die Erweiterungen.
Das wäre so weit plausibel, ich befürchte aber, dass das Gegenteil passieren würde, also dass der Überwachungsauftrag erweitert wird, weil nichts Erhärtendes gefunden wird. In den Ermittlungsakten zu Andrejs Terrorismus-Verfahren gab es keine Online-Durchsuchung, die war damals noch gar nicht beschlossen. Aber es gab Überwachungsbeschlüsse, die erweitert wurden, etwa die Telefon-Überwachung betreffend. Und eben nicht, weil vorher etwas mitgehört worden wäre, das den Verdacht bestätigt hätte. Verdächtig war, dass nichts verdächtig war. Dann, so die Logik der Überwachenden, musste der Beschuldigte sich ja wohl besonders konspirativ verhalten. Ergo: Die ist sowieso alles öffentlich.“ Im Umkehrschluss bedeutet das: Wer die Offenbarung der eigenen Identität verweigert, hat noch eine Leiche im Keller. Nach der dringend mal geschaut werden muss.

Dieses Argument setzt voraus, dass Beobachtung grundsätzlich wohlwollend stattfindet. Und das ist ja nun mal leider nicht immer der Fall. Das Perfide an Terrorismus-Ermittlungen ist, dass nur zum Teil nach Beweisen gesucht wird, die eine konkrete Tatbeteiligung belegen. Eine mindestens so große Rolle spielt die zu beweisende Mitgliedschaft in einer terroristischen Vereinigung, die in der Regel keine Mitgliedsausweise ausstellt. Es geht also – um ein angestaubtes Wort zu bemühen – um Gesinnung. In Andrejs Fall haben wir zig Beispiele gefunden, in denen BKA und Staatsanwaltschaft die Ergebnisse der Überwachung in einer Weise interpretiert haben, wie wir unser Leben gar nicht gelebt haben.

Als Andrej im Zeitraum der Überwachung überlegte, sich auf eine Stelle in den Niederlanden zu bewerben, wurde er am Telefon gefragt, was wir, seine Familie, denn dann täten. Aus seiner Antwort, dass er möglicherweise für ein paar Wochen oder Monate allein dort leben würde, bis wir nachzögen, wurde in einem Schriftstück der Staatsan-

Eine Folge davon war, dass noch mehr Menschen zu Betroffenen wurden, denn wer mit potenziellen Terroristen Kontakt hat, wird auch überprüft und landet in der einen oder anderen Datenbank.

OB DIE WIEDER WEG SIND, KANNST DU GAR NICHT WISSEN

Selbst jetzt noch, Jahre nach der Verhaftung, ein gutes Jahr nach Einstellung des Verfahrens, kann ich nicht ausschließen, dass der Verfassungsschutz weiter ein Auge auf uns hat. Es bedarf keiner besonderen Fantasie, um sich auszudenken, dass per Online-Durchsuchung auf verdächtigen Computern gefundene Namen, Bilder, E-Mail- oder Chat-Kontakte auch ins Raster geraten. Terrorismus ist einer der Straftatbestände, die die Online-Durchsuchung rechtfertigen.

Wie viele Terrorismus-Verfahren in Deutschland geführt werden, ist unbekannt, von den meisten erfahren die Beschuldigten nie: Sie werden nach Monaten und Jahren der Überwachung ergebnis-, aber für die Betroffenen eben nicht folgenlos eingestellt. In den Akten zu Andrejs Verfahren werden neben den Beschuldigten mehr als 200 Personen genannt.

Layout: Christine Zander. Vertrieb: Michael Balke, vertrieb@denkselbst.org. Finanzen: Volker Neubert, Post an Kompass/DenkSelbst e.V. z.H.Volker Neubert, Hackenbroicher Weg 24, 50259 Pulheim

DAS POLITISCHE GESPRÄCH: KOMPASS – INTERVIEW MIT UDO VETTER

PRISM IST DEIN ARBEITSPLATZ

BUNDESTAGSKANDIDAT UDO VETTER ZUM NSA-SPÄHPROGRAMM „PRISM“

Udo Vetter ist ein deutscher Rechtsanwalt und Strafverteidiger, Lehrbeauftragter der Fachhochschule Düsseldorf und Autor des auch jenseits von juristischen Kreisen wohlbekannten „law blog“ (http://www.lawblog.de/). Bekannt wurde er durch seine zahlreichen Interviews und Auftritte als Rechtsexperte. Seit April 2012 ist Udo Vetter Mitglied der Piratenpartei.

Kompass:
Udo, Du hast in einem Gespräch vor kurzem gesagt: „PRISM ist Dein Arbeitsplatz“!Was genau meinst Du damit?

Udo Vetter:
Die Empörung über PRISM richtet sich derzeit gegen die Auswirkungen, welche die laufende Totalüberwachung auf das Privatleben der Menschen hat. Völlig zu Recht, denn ein überwachter Mensch ist nicht frei.

Neben den Bürger- und Freiheitsrechten stehen jedoch auch Arbeitsplätze auf dem Spiel. Ein Motiv für Spionage ist es seit jeher, an Betriebsgeheimnisse ausländischer Unternehmen zu kommen.

TOTALE WIRTSCHAFTS-SPIONAGE

Es wäre lebensfremd zu glauben, die US-Regierung interessiere sich nicht für Daten aus deutschen Unternehmen. Wer den kompletten Internetverkehr abschnorchelt, kriegt logischerweise auch kompletten Zugriff auf sensible Firmendaten, von der einfachen Kundenliste bis zu den Plänen für ganze Industrieanlagen.

All das landet in den USA und findet seinen Weg. Um das zu sehen, muss man kein Verschwörungstheoretiker sein. Der deutsche Mittelstand und darunter besonders die Maschinenbauer, die uns Exportweltmeistern machen, tun sich schwer damit, ihre elektronische Kommunikation auf NSA-Niveau zu sichern. Ich glaube nicht mal, dass dies den großen deutschen Konzernen gelingt. Selbst dort ist mittlerweile die Verzweiflung groß, wie ich von unterschiedlichen Bekannten in Führungspositionen weiß.

Kompass:
Was können wir im Bundestag gegen diese Ausspähung tun?

Udo Vetter:
Es wird unsere Aufgabe sein, der Regierung den nötigen Druck zu machen. Wir sind die einzige Partei, die konsequent nicht nur das Internet als „zweiten Lebensraum“ verteidigt, sondern die Freiheits- und Bürgerrechte insgesamt. SPD und Grüne haben in diesem Punkt faktisch versagt. Sie machten in der Vergangenheit oft schöne Worte, in der Regierungsverantwortung taten sie aber das Gegenteil. Und selbst heute sprechen sich diese Parteien noch für eine Vorratsdatenspeicherung aus. Sie sind längst dem Sicherheitswahn erlegen.

Kompass:
Wie soll Deutschland / Europa reagieren?

Udo Vetter:
Es wäre toll, wenn Deutschland überhaupt etwas täte. Aber die Regierung erweckt den Eindruck, als finde sie die Abschaffung unserer Freiheit so wichtig wie eine neue EU-Gemüseverordnung – für beides interessiert die Kanzlerin sich ja nach eigenem Eingeständnis nicht.

KEIN DATEN-AUSTAUSCH MEHR

Dabei könnten wir uns wehren, nicht nur können, wir müssen es sogar. Der Austausch von Überweisungs- und Fluggastdaten sollte gestoppt werden. Der NSA muss ein „Betriebsverbot“ in Deutschland erst angedroht und dann notfalls auch auferlegt werden. Wirtschaftlicher Druck wäre dadurch möglich, dass Daten aus der EU nicht mehr von US-Firmen gespeichert werden dürfen.

Das ginge durch Aufkündigung des Safe-Harbour-Abkommen (http://de.wikipedia.org/wiki/Safe_Harbour). So fordern es ja mittlerweile auch die Datenschutzbeauftragten der Länder. Sowohl auf EU- als auch in Deutschland-Ebene sind Untersuchungsausschüsse erforderlich. Wir haben Anspruch auf Klarheit.

Und noch eins: Deutschland sollte Edward Snowden eine Aufenthaltserlaubnis anbieten. Dazu ist die Bundesregierung durchaus berechtigt, so steht es klar im Aufenthaltsgesetz. Beispielsweise erhalten jetzt afghanische BND-Informanten ein Bleiberecht in Deutschland. Dieses Beispiel zeigt, dass im Fall Snowden mit falschen Karten gespielt wird.

Kompass::
Was können Wähler von Ihrem Bundestagsabgeordneten Udo Vetter erwarten?

Udo Vetter:
Ich werde darum kämpfen, dass das Grundgesetz nicht nur in Sonntagsreden lebendig bleibt. Ich möchte, dass meine Patenkinder auch noch erfahren, wie sich Freiheit anfühlt.

Kompass::
Udo Vetter, vielen Dank für das Gespräch.

Wer nichts zu verbergen hat ist nackt.
Ich sehe allerdings keine Nackten auf der Straße.

(Ulrich Scharfenort, 31.07.2013)

Immer wieder hört man: wer nichts zu verbergen hat, braucht die Überwachung der kommerziellen Anbieter oder Schnüffelstaaten nicht zu fürchten.

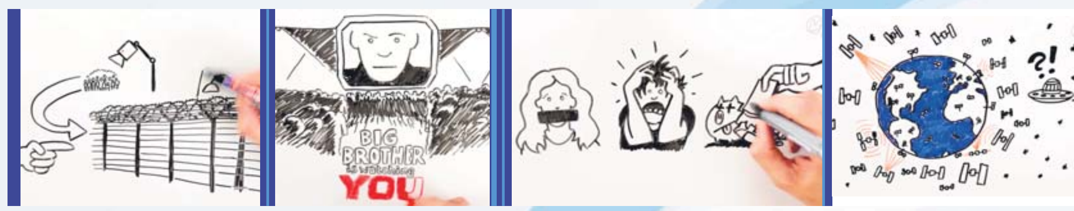
Seltsam ist nur, dass **jene,** die so etwas predigen, **besonders viel zu verbergen haben.** Seien es Politiker, die ihre Nebeneinkünfte nicht lückenlos aufdecken oder Konzerne die bestimmt keine Privatpersonen dulden würden, die dort in firmeninternen Papieren lesen wollen.

In Wirklichkeit zeigt diese Behauptung nur, **dass jeder etwas zu verbergen hat.** Sei es nur die eigene Privatsphäre vor den wachsamen Augen von Big Google & Co., die auch die kleinste Datenressource kommerziell verwerten wollen. Nicht nur in Form von personalisierten Werbebannern. Schon heute kann viel mehr gemacht werden, mit den Daten über eine Person.

Vielleicht erscheint vieles jetzt sogar noch als Spielerei, aber das ist heute und kann sich innerhalb weniger Jahre schnell in einem Albtraum verwandeln. Wer heute die Privatsphäre verteidigt, **verteidigt auch die Zukunft** und konzernokratische Unabhängigkeit von morgen.

KRYPTOPARTYS VERSUS NSA, PRISM, TEMPORA UND CO.?!

WIR werden seit Jahren umfassend ausspioniert, durch die USA, Großbritannien und wer weiß von wem noch. Was viele Computerexperten seit langem vermuteten, wurde jetzt zur Gewißheit: dank Edward Snowden



Die NSA und andere Geheimdienste sammeln ungehemmt unsere Daten. „Nur" für die Terrorabwehr und Terroristenaufspürung oder auch um Wirtschaftsspionage „nebenbei" zu betreiben? Ich will ungestört kommunizieren können, ohne dass ein Big Brother alles sammelt. Zu verbergen habe ich das Gleiche, wie jeder andere hier auf diesem Planeten: Meine Privatsphäre. Was ich wann, wie, wo, wem und warum schreibe, rede oder handle ist meine Sache. Meine Äußerungen sind natürlich auch immer abhängig von meinen Gefühlen. Mit einem entsprechenden Such-Algorithmus und Interpretation ist es möglich, selbst aus einem Gandhi einen Diktator hinzubasteln. Doch warum sollte dies Herr Regi Erung jemals mit Herrn Bür Ger tun? Nun, dann wenn er unbequem wird. Die Piratenpartei setzt sich (seit Jahren) gegen solche massiven Bevölkerungsüberwachungen ein. Doch was tun? Sind wir alle den Geheimdiensten hilf- und schutzlos ausgeliefert? Nein, es gibt Lösungen, die teilweise sogar schon seit Jahrzehnten existieren!

Als da wären...

FORTBILDUNG
Eine Kryptoparty besuchen, sich im Internet informieren oder/und diesen Artikel weiterlesen.

INTERNET
Anonym im Internet surfen (etwa mit TOR oder über ein verschlüsseltes Virtuelles Privates Netz (VPN) wie https://www.hide.io).

E-MAILS
E-Mails nur SSL-verschlüsselt senden, zum Beispiel mit https://posteo.de oder per PGP.

SUCHMASCHINEN
Nur diskrete Suchmaschinen verwenden (zum Beispiel https://www.ixquick.de)

FESTPLATTEN/SPEICHERMEDIEN RICHTIG LÖSCHEN
Entweder über die Gutmann-Methode oder mittels Feuer (meine bevorzugte Methode bei meinen gebrauchten Festplatten, die ich nicht mehr benötige).

FESTPLATTEN VERSCHLÜSSELN
Zum Beispiel mit dem Programm TrueCrypt (dies ist jedoch unter gewissen Umständen knackbar, also nicht absolut sicher), BitLocker etcetera.

DATENVERSCHLÜSSELUNG UND PASSWÖRTER
Date(i)en können durch Komprimieren, mit einem Passwort versehen und einem AES 128-Bit-Schlüssel sicher verschlüsselt werden! Das funktioniert auch mit den aktuellen Versionen von WinZip und WinRAR. Die erzeugten Archive können nur mit dem richtigen Passwort entpackt werden. Um ein einfaches Ausprobieren durch Computer zu erschweren, darf das Passwort nicht zu kurz sein, keine Wörter enthalten, und sollte aus Klein-, Großbuchstaben, Zahlen und Sonderzeichen bestehen. Ein ungeeignetes Passwort wäre: MeersandVentilator35Hasenohren. Durch eine Änderung des Passworts in M€€rs@ndV€ntil@tor35H@s€nohr€n wird das Passwort nicht besser, da solche Schreibvarianten bekannt sind und ebenfalls durchprobiert werden. Ein sehr gutes Passwort wäre: jZ4590%rfT@]9^3909fsWT/swüß?

Wichtig: keinem das Passwort sagen und es nicht notieren!

WARUM IST DIE LÄNGE SO ENTSCHEIDEND?
Jedes Zeichen des Passworts hat (theoretisch) 255 Darstellungsmöglichkeiten. Daher ist es wichtig sehr verschiedene Zeichen aus einem Zeichensatz zu nehmen und zum Beispiel nicht nur Zahlen. Sonst gibt es statt 255 plötzlich nur noch 10 Möglichkeiten je Zeichen. Für einen sehr schnellen Computer ist es möglich, 800 Milliarden Passwörter in der Sekunde zu erstellen. Sein Problem ist jedoch, dass er es nicht schafft, 800 Milliarden Passwörter in der Sekunde auch auszuprobieren.

WIE LANGE BENÖTIGT EIN COMPUTER FÜR EIN ZWANZIGSTELLIGES PASSWORT?
Gehen wir einmal davon aus, dass es möglich wäre, 1 Billion Passwörter in der Sekunde zu erstellen und auszuprobieren. Um es einfacher zu rechnen nehmen wir nur 100 (statt 255) verschiedenen Darstellungsmöglichkeiten je Zeichen an und berücksichtigen nicht, dass der Computer auch alle ein- bis neunzehnstelligen Passwörter ausprobieren muss - da ja nicht bekannt ist, wie lange das Passwort ist. Bei einem einstelligen Passwort gibt es 100 Möglichkeiten, bei einem zweistelligen Passwort 100 x 100 (= 10.000) Möglichkeiten, bei einem dreistelligen Passwort 100 x 100 x 100 Möglichkeiten und so weiter. Bei einem zwanzigstelligen Passwort ergibt dies also 100 hoch 20 (= 1 Septillion) Möglichkeiten. Eine Septillion geteilt durch eine Billion geteilt durch 31.536.000 Sekunden (entspricht einem Jahr) ergibt 317.098.000.000.000.000.000 Jahre, die der Computer maximal benötigen wird, um das Passwort zu knacken. Wahrscheinlich benötigt er jedoch „nur" die halbe Zeit, da es unwahrscheinlich ist, dass erst der letzte Versuch das richtige Passwort ist. Wenn ein Computer in über 150 Trillionen Jahren das Passwort endlich geknackt hat, dürfte es dem Ersteller so ziemlich egal sein. Selbst wenn eine Million Supercomputer parallel arbeiten, benötigen sie wohl immer noch so um die 150 Billionen Jahre. Natürlich dauert es deutlich länger, da es ja jeweils 255 Möglichkeiten je Zeichen gibt und der/die Computer auch die Passwortlängen vorher ausprobieren muss.

Aber ich wollte die Zahlen eben etwas überschaubarer halten.

WEITERFÜHRENDE LINKS
http://www.password-depot.de/know-how/brute_force_angriffe.htm
http://www.distributed.net/RC5/de
http://kryptoparty.de/

AES 128-BIT-SCHLÜSSEL

Advanced Encryption Standard, auch Rijndael-Algorhitmus genannt, bietet ein extrem hohes Maß an Sicherheit. Es ist ein symetrisches Kryptosystem, das seit über zehn Jahren Standard ist. Weiteres unter: http://de.wikipedia.org/wiki/Advanced_Encryption_Standard

BRUTE-FORCE-ANGRIFF

Ein Brute-Force-Angriff (Übersetzung: Roher-Gewalt Angriff) bezeichnet das bloße Ausprobieren aller (oder möglichst vieler) Passwörter. Kennt man die Passwortlänge und die maximal verfügbaren Darstellungsmöglichkeiten, lassen sich die maximal möglichen verschiedenen Passwörter einfach errechnen. Auch deswegen ist es sehr wichtig, dass niemand die Passwortlänge (außer natürlich dem Benutzer selbst) kennt. Denn weiß der Angreifer, dass es 15 Stellen hat, braucht er keine Zeit an alle 1 bis 14-stelligen Passwörter verschwenden.

DICTIONARY-ANGRIFF

Ein Dictionary-Angriff (Wörterbuch-Angriff) ist oft die erste Wahl, um ein Passwort zu knacken, was daran liegt, dass es (im Vergleich zu irgendwelchen Buchstaben, Zahlen, Sonderzeichen-Kombinationen) nur wenige Wortkombinationen gibt. Der Wortschatz der deutschen Sprache umfasst etwa 300.000 bis 500.000 Wörter, der englischen Sprache etwa 500.000 bis 600.000. Bei einem einfachen Dictionaryangriff versucht der Computer alle möglichen Wortkambinationen, bei einem erweiterteten Dictionaryangriff mischt er zum Beispiel noch ein paar Zahlen, andere Schreibweisen (H@s€ oder HaS€ statt Hase) rein, kombiniert wahrscheinliche Sprachmischungen (Deutsch und Englisch oder Deutsch und Französich) und und und. Die Erweiterungen können individuell angepasst werden, je mehr, desto mehr Möglichkeiten gibt es. Deswegen ist ein Passwort wie ReG€ncarwash37Köln) nicht so sicher, wie es erscheint. Ein ordentlicher Hacker benötigt mit dem entsprechenden Programm, Hintergrundwissen der Person und einem etwas schnelleren PC dafür vermutlich noch nicht einmal einen Tag. Sollte es sich um eine WinZIP- oder WinRAR-Datei handeln, wird er deutlich länger brauchen (vielleicht 30 Tage), das ist jedoch immer noch kurz genug, um dem Benutzer schaden zu können.

GUTMANN-METHODE

Der Benutzer hat seine, ihm sehr wichtigen, Daten nun ordentlich mit WinRAR verschlüsselt, auch beim Passwort hat er an alles gedacht und löscht nun die unverschlüsselten Originaldaten. Doch er muss sie richtig löschen. Bei einer Magnetfestplatte empfiehlt sich die sogenannte Gutmann-Methode, das heißt, der Festplattenbereich wird nach einem bestimmten Muster bis zu 35-mal überschrieben. Bei einer SSD-Platte, einem SD-Stick oder USB-Stick reicht ein einmaliges Überschreiben, da dies die entsprechenden Bereiche tatsächlich löscht! Es gibt freie Programme (zum Beispiel Secure Eraser), die es ermöglichen, den kompletten freien Speicher der Festplatte sicher zu löschen, so dass Daten durch einen möglichen Restmagnetismus auch wirklich nicht mehr herzustellen sind. Um zu schauen, welche gelöschten Dateien wiederherstellbar sind, kann der Benutzer einfach das kostenlose Programm Recuva ausprobieren.

TOR

Nein, hier geht es nicht um Fußball, sondern um das The Onion Router / Routing. Aber was hat eine Zwiebel (englisch Onion) mit Computer und Sicherheit zu tun? Nun, sehr viel. Die Zwiebel steht quasi als Symbol für die Arbeitsweise des Routers. Eine Zwiebel besteht aus sehr, sehr vielen Schichten. Und etwa das passiert, wenn ein Benutzer mit TOR in das Internet geht. Sie gehen verschlüsselt über mehrere Server (mindestens drei) zufällige Wege kreuz und quer und sind (sofern Sie noch ein paar Programmeinstellungen berücksichtigen) sehr sicher und anonym im Internet unterwegs. Sie zwiebeln sich quasi durch das Netz.

PGP

PGP steht für Pretty Good Privacy, also sinngemäß für ziemlich gute Privatsphäre
Es gibt zwei Schlüssel, einen öffentlichen und einen privaten, geheimen Schlüssel. Beide Schlüssel zusammen ergeben ein eindeutig zuzuordnendes Schlüsselpaar. PGP ist ein sehr sicheres Verfahren und wurde bereits 1991 (!!!) von Phil Zimmermann entwickelt, um Bürger vor der Schnüffelei durch die Geheimdienste zu schützen!

KRYPTODISC ZUM DOWNLOADEN

http://downloads.cheatha.de/cryptodisk/cryptodisk_0.19_1.iso

VPN

VPN steht für Virtuelles Privates Netz
Sehr vereinfacht ausgedrückt ist ein VPN eine Softwarelösung, damit geschlossene private Netze untereinander kommunizieren können. Durch eine Verschlüsselung ist zudem eine manipulations- und abhörsichere Verbindung möglich.

Wird eine VPN-Verbindung über einen Computer aufgebaut, so ändert sich die ursprüngliche IP-Adresse in die IP-Adresse des VPN, ebenso verändert sich das Routing. Mit VPN ist ein sehr sicheres und anonymes Surfen im Internet möglich!

2013.NSA

KOMPASS

//kompass.im

Demokratie und Freiheit, Bürgerrechte und informationelle Selbstbestimmung, Transparenz in Politik und Staat, existenzielle Sicherheit und gesellschaftliche Teilhabe, freier Zugang zu Information und Bildung, ein bürgerfreundliches Urheber- und Patentrecht, sowie weitere Themen, die Piraten bewegen

NSA: WIR KENNEN DEINE GEHEIMNISSE!

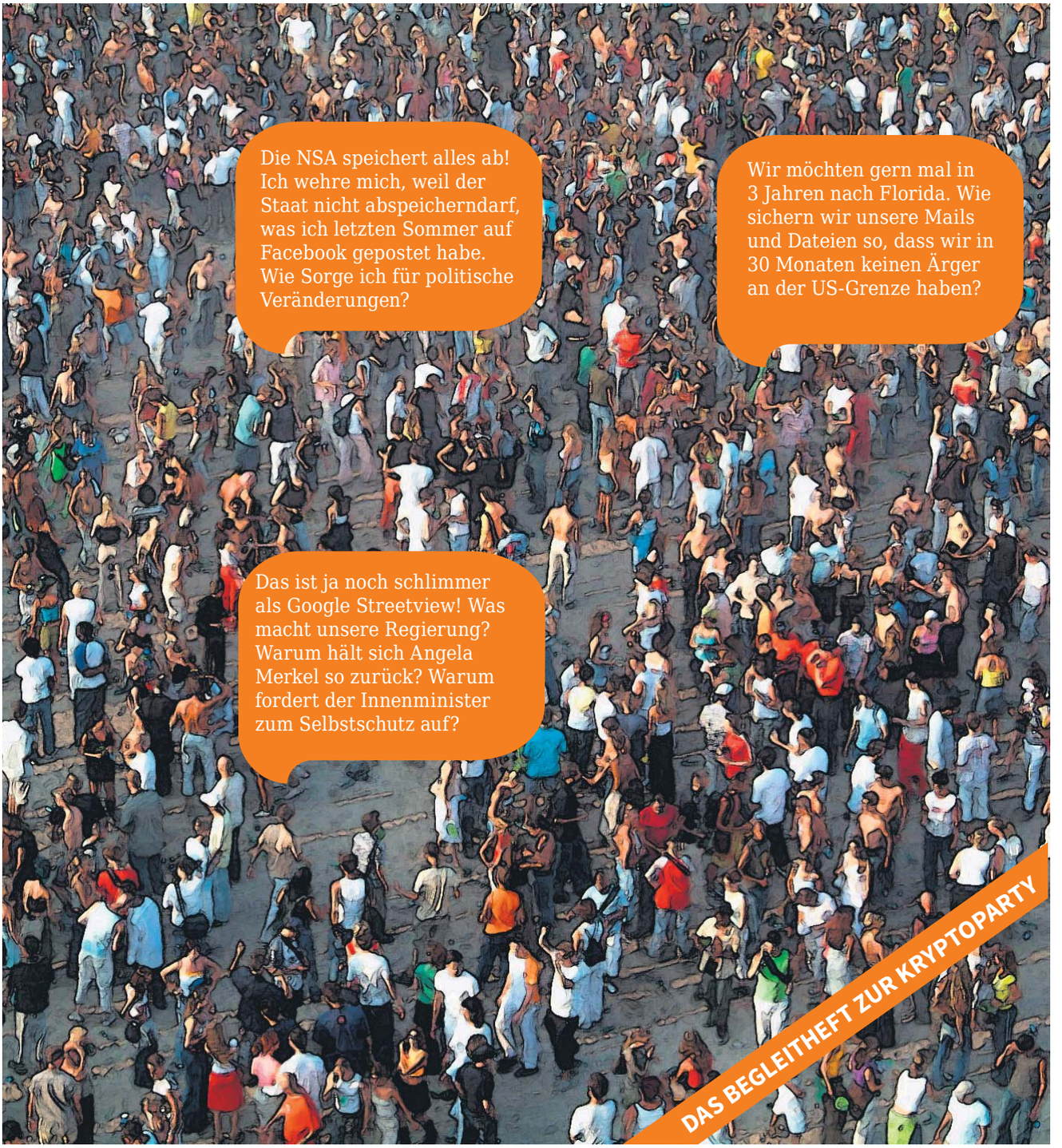
FREIHEIT STATT ANGST UND ÜBERWACHUNG

2013.NSA

KOMPASS

//kompass.im

Demokratie und Freiheit, Bürgerrechte und informationelle Selbstbestimmung, Transparenz in Politik und Staat, existenzielle Sicherheit und gesellschaftliche Teilhabe, freier Zugang zu Information und Bildung, ein bürgerfreundliches Urheber- und Patentrecht, sowie weitere Themen, die Piraten bewegen



NSA: WIR KENNEN DEINE GEHEIMNISSE!

FREIHEIT STATT ANGST UND ÜBERWACHUNG

2013.NSA

KOMPASS

//kompass.im

Demokratie und Freiheit, Bürgerrechte und informationelle Selbstbestimmung, Transparenz in Politik und Staat, existenzielle Sicherheit und gesellschaftliche Teilhabe, freier Zugang zu Information und Bildung, ein bürgerfreundliches Urheber- und Patentrecht, sowie weitere Themen, die Piraten bewegen

NSA: WIR KENNEN DEINE GEHEIMNISSE!

FREIHEIT STATT ANGST UND ÜBERWACHUNG