Mobbing durch die Dienste

Weitere Dokumente Snowdens zeigen (via Fefe), dass die Geheimdienste missliebige Personen gezielt verunglimpfen und mobben, ja sogar kompromittierende Dateien versuchen auf deren Rechner zu schmuggeln.

Die Methode, jemanden zu diskreditieren, kenne ich übrigens schon von der Stasi („Zersetzung nach Plan„), von den üblichen Bekloppten online und vom verbandsinternen Mobben im DJV, nur dass Verbandsfunktionäre meistens zu blöd sind, um einen Rechner effektiv zu nutzen.

Asozial ohne Facebook

„Der 22-jährige Sven B. wurde heute zwangsweise in die Psychiatrie eingewiesen, weil er keinen Account bei dem sozialen Netzwerk Facebook hat. Zuvor hatten Freunde die Gesundheitsbehörden alarmiert, weil sie sich wegen des asozialen Verhaltens des jungen Mannes große Sorgen machten.“ (Quelle)

Bandenmässiger Betrug unter Beteiligung von Juristen

Aus dem Heise-Forum:

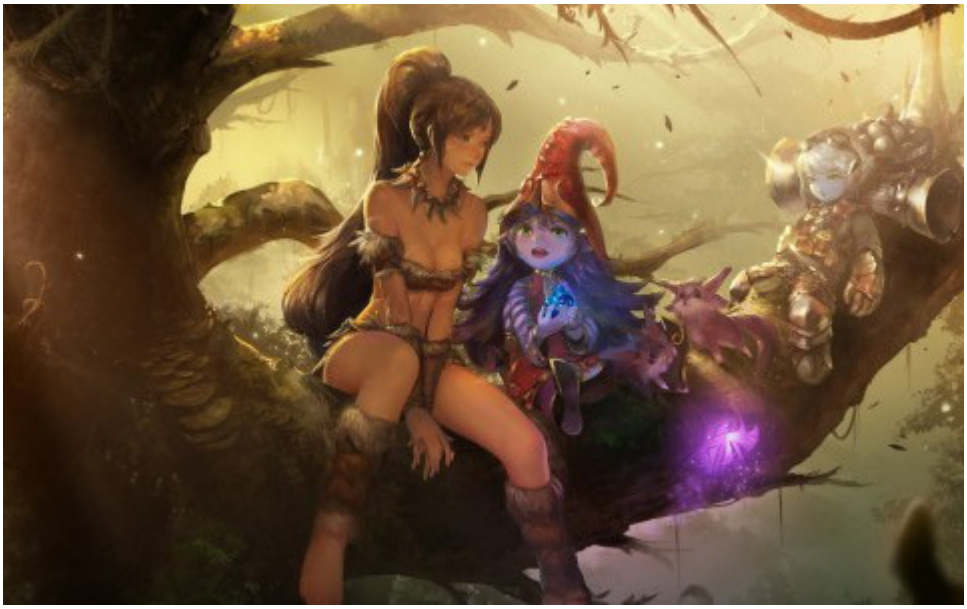
Richter geben dem Eingiff in die Rechte unbescholtener Personen statt, weil eine Briefkastenfirma über ein PHP Script mitloggen kann, dass ein Browser einen Stream startet, dessen Nutzungsrechte eine Firma für sich proklamiert und weil sich ein Anwalt findet, der bereit ist den Anschlussinhaber dafür abzumahnen, dass ein Browser gestartet wurde, der dank Trafficredirection auf einem Server mit einem PHP-Script gelandet ist, der einen Datenstrom weiterleitet dessen Empfang eigentlich nicht abgemahnt werden kann, weil es kein Download ist und der Abmahnende auch gar nicht die für die Abmahnung benötigten Rechte an dem Werk besitzt, was höchstwahrscheinlich ohnehin irrelevant wäre, da Pornos nur „den sexuellen Akt zeigen“ und ihnen somit die Schöpfungshöhe fehlt, die nötig wäre um das Werk schützenswert zu machen.
Angesichts dieser Umstände bleibt nur die Frage, in wie weit es sich bei der Tätigkeit von Juristen um geistige Onanie handelt und falls ja, ob die Berufsbezeichnung Jurist, dank der dann fehlenden Schöpfungshöhe überhaupt schützenswert ist.

Bandenmässiger Betrug, § 263 StGB:
(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter
1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Urkundenfälschung oder Betrug verbunden hat,
2. einen Vermögensverlust großen Ausmaßes herbeiführt oder in der Absicht handelt, durch die fortgesetzte Begehung von

Betrug eine große Zahl von Menschen in die Gefahr des Verlustes von Vermögenswerten zu bringen,
3. eine andere Person in wirtschaftliche Not bringt,

Meines Erachtens trifft das auf viele „Massenabmahnanwälte“ zu, die sich auf das Urheberrecht berufen. Und man sieht, welchen Abschaum die heilige Kuh des Kapitalismus im Zeitalter des Internet auf den Plan ruft.

VarusExpirationTimer.luaobj



Pornoanwalt: „League of Legends (LoL) zählt zu den umsatzstärksten Free-to-Play-Spielen im Jahr 2013. Nun wurde bekannt, dass britische Spieler auf das letzte Update von League of Legends verzichten mussten, denn der Pornofilter des Landes verhinderte den Download“.

Was sagen eigentlich die oberste deutsche Zensurbehörde, jugendschutz.net und Alice Schwarzer zu diesem Thema?

Tor, the bad guys and the good guys

Heise: „Forscher von der schwedischen Karlstad University sind bei einer systematischen Analyse des Tor-Netzwerks (PDF) auf 20 Exit-Nodes gestoßen, die verschlüsselte Verbindungen angreifen.“
Several hundred Tor exit relays together push more than 1 GiB/s of network traffic. However, it is easy for exit relays to snoop and tamper with anonymised network traffic and as all relays are run by independent volunteers, not all of them are innocuous. (…) To reduce the attack surface users are exposed to, we further discuss the design and implementation of a browser extension patch which fetches and compares suspicious X.509 certificates over independent Tor circuits. Our work makes it possible to continuously monitor Tor exit relays.

Sie werden platziert

Schadprogramme platzieren sich unbemerkt auf dem Rechner eines Opfers. (Abbildung ähnlich)

Bundesamt für Sicherheit in der Informationstechnik (BSI) :
„Die Schadprogramme werden unbemerkt auf den Rechnern der Anwender platziert, um beispielsweise Tastatureingaben und Anmeldevorgänge zu protokollieren oder Transaktionen direkt zu manipulieren.“

Unbemerkt. Platziert. Darf ich, bitte, fragen, wie? Auf meinen Rechnern? Unbemerkt? Per Voodoo? Oder vielleicht durch ein höheres Computerwesen?

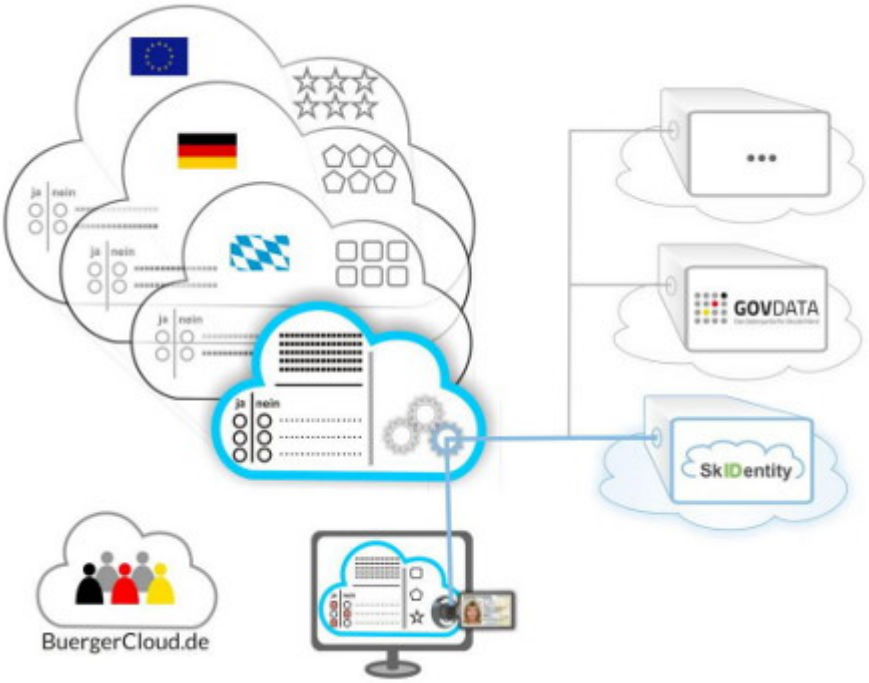
Gangbang, Gender und Mobilgeräte für Kinder

Don Alphonso: „Da gibt es nämlich so Videoseiten im Internet, die durch ihr internationales Publikum dafür sorgen, dass Fachtermini auf Englisch Einzug halten. Nie also steht dort etwas von Gruppensex, sondern immer nur von Gangbang, und meine Befürchtung ist nun, dass so mancher Lehrer in seinem geordneten Leben vielleicht gar nicht so richtig erfasst, welche neuen Möglichkeiten das Internet zugänglich macht. Was dann bei Twitter wiederum die Erkenntnis reifen lässt, dass es nach dem Abbruch der Schule auch eine Karriere als Pornoaktrice geben könnte. In derjenigen Perversion, die am besten zu den weithin ausgebreiteten körperlichen Nachteilen der Autorin passt. Natürlich liest so etwas kein Pfarrer aus Tübingen und keine Feministin in Berlin und Eltern lesen das auch nicht, sonst hätte das Kind nämlich kein Mobilgerät mehr…“

Schön ist auch diese Karte – wie Kinder sich heute bewegen bzw. nicht bewegen.

The Day We Fight Back

In der Bürgerwolke



Screenshot: Gutachten: Universität Passau, Lehrstuhl für Öffentliches Recht und ecsec GmbH: Eine „BürgerCloud“ für mehr Partizipation – Rechtliche Rahmenbedingungen und Ansätze zur Umsetzung

Ich habe mir das von Heise zitierte Gutachten der Universität Passau über „Online-Wahlen“ einmal genauer angesehen. Es ist natürlich einfach, die Bürokraten, die sich pseudo-Technik-affine Begriffe wie „ePerso“, „Bürgercloud“, „eID-Broker“ und „SkiIdentity“ ausdenken, mit Häme zu überschütten. Da reden Blinde von Farben, und sie meinen es noch nicht einmal gut. Zum Glück gibt es klare Vorgaben des Bundesverfassungsgerichts, wann Wahlen noch demokratisch sind. Die zitiert das Gutachten auch [*die Links musste ich selbst zusammensuchen*]:

Jenseits der bisher noch eher theoretischen Frage, ob bestimmte Vorstellungen einer Liquid Democracy mit den konkreten Vorgaben des Grundgesetzes (beispielsweise der Unabhängigkeit von Mandatsträgern) kollidieren, hat das Bundesverfassungsgericht [BVerfG09] insbesondere in der Entscheidung zu elektronischen Wahlgeräten Grenzen für den

Einsatz von Informations- und Kommunikationstechnik bei staatlichen Wahlen und Abstimmungen gezogen (dazu z.B. [BuRo09], [Rich12]; zur Weiterentwicklung bzgl. Internetwahlen auch [BGRR13]).

Das Gericht leitet aus Art. 38 Abs. 1 i.V.m. Art. 20 Abs. 1 und Abs. 2 GG den Grundsatz der Öffentlichkeit der Wahl ab: jeder Wähler muss die Möglichkeit haben, sich selbst zuverlässig von der Rechtmäßigkeit des Wahlakts zu überzeugen. Dazu müssen die wesentlichen Schritte der Wahl ohne besondere technische Vorkenntnisse nachvollziehbar sein.

Online-Wahlen werden also, wie auch die Gutachter zugeben „in Deutschland bis auf weiteres auf Vereine, Aktiengesellschaften, Kirchen und andere nichtstaatliche Institutionen beschränkt bleiben“. Ich habe bekanntlich das Piraten-Projekt Liquid Feedback für eine Totgeburt gehalten und bin dafür übel beschimpft worden; aber ich habe natürlich recht gehabt und behalten. Bei einer der nationalen Minderheiten Deutschlands gibt es, soweit ich weiß, aber noch keine Beschwerden über das Procedere.

In Vereinen sind Online-Wahlen mittlerweile gang und gäbe, aber man muss gewährleisten, dass alle, die teilnehmen, sich eindeutig identifizieren können und jeder Zugang hat. Bei Vereinen ist das kein Problem, da die ihre inneren Angelegenheiten weitgehend selbst gestalten dürfen und etwas nur vor Gericht landet, wenn sich jemand beschwert und der interne Beschwerdeweg ausgeschöpft worden ist. Im Gutachten heißt es:

Die durch das Bundesverfassungsgericht aufgestellten Beschränkungen gelten dem Grunde nach auch für Abstimmungen (Bürgerentscheide). Das Gericht hat aber keine Aussagen für sonstige direktdemokratische und partizipative Mechanismen getroffen.

Da liegt der Hase im Pfeffer bzw. schwebt der Bürger in der

Bürgerwolke. Wenn Online-Wahlen per „sicherer“ Bürgercloud sich erst eingebürgert haben, dann wird es einen neuen Versuch à la Söder geben, Wahlen insgesamt durch „sichere“ Technik machen zu lassen. Eine Alternative sieht das Gutachten im Umweg über die EU:

Damit der neue Personalausweis und ähnliche europäische Ausweiskarten in einer effizienten Art und Weise in der BürgerCloud genutzt werden können, soll (…) der im SkIDentity-Projekt entwickelte eID-Broker eingesetzt werden. Die Unterstützung der Ausweiskarten unserer europäischen Nachbarn ist wichtig, da elektronische Bürgerbegehren in der Europäischen Union eine besondere Bedeutung erlangen könnten. Denn hier ermöglicht Art. 11 Abs. 4 EUV seit dem Vertrag von Lissabon ein europäisches Bürgerbegehren [GoAs11]: Wenn sich mindestens eine Million Unionsbürger aus einer „erheblichen Anzahl von Mitgliedstaaten“ zusammenfindet, können sie die Europäische Kommission auffordern, im Rahmen ihrer Befugnisse geeignete Vorschläge zu unterbreiten, die in Rechtsakte der Union münden können.

Einschränkend muss man sagen, dass das oben zitierte Gutachten als Thema zunächst Bürgerbegehren in Bayern hatte, und primär die dortigen Landesgesetze untersucht, ob sie für Online-Wahlen etwas taugen. Und diejenigen, die sich an „Online-Petitionen“ beteiligen, sollten nicht jammern. Dort bestehen alle Probleme, die gegen Online-Wahlen sprechen, jetzt schon:

Art. 2 Abs. 1 Satz 3 bis 5 BayPetG regelt die Voraussetzungen einer zulässigen OnlinePetition zum Bayerischen Landtag. Neben der elektronischen Form ist danach die Schriftform gewahrt, wenn der Urheber und dessen Postanschrift ersichtlich sind. Zudem muss das im Internet zur Verfügung gestellte Formular verwendet werden, in das neben Name und Adresse eine gültige E-Mail-Adresse des Petenten eingetragen werden muss. Die weitere Kommunikation kann dann per E-Mail stattfinden. Eine Überprüfung der Identität erfolgt nicht.

Online-Petitionen in Bayern kann man also leicht fälschen und verfälschen. Zur „Bürgercloud“ ist das Gutachten auch sehr vorsichtig:

Die Nutzung einer Infrastruktur, die ganz oder teilweise nicht zumindest innerhalb der EU oder des EWR angesiedelt ist, scheidet im Bereich sensibler, auf Partizipation und hoheitliche Gewalt ausgerichteter Verarbeitung personenbez ogener Daten dabei von vornherein aus …

Meine These: Wenn man die Details des Gutachtens liest und auch dessen Zusammenfassung, suggerieren die Juristen, dass der Staat eine Art mobile Wahl-Technik zur Verfügung stellen soll, um Kosten zusparen: „es können entsprechende Dienste von einem dafür spezialisierten Anbieter in einem Software-as-a-Service-Modell bezogen werden.“

Schon klar. Am besten von Microsoft in Kooperation mit Siemens oder der Telekom. Das obige Gutachten stammt ja auch schon teilweise von einer Firma. Ersec ist ein „spezialisierter Anbieter von innovativen Lösungen im Bereich Sicherheit in der Informations- und Kommunikationstechnologie, Sicherheitsmanagement, Chipkartentechnologie, Identitätsmanagement, Internetsicherheit und Elektronische Signatur.“ Der Hinweis, dass das Gutachten nicht wissenschaftlich unabhängig ist, fehlt leider bei Heise.

Das Ende der Demokratie ist nahe

Söder (CSU) aus Bayern möchte Wahlen fälschen können. Estland hat die Erfahrungen schon gemacht.

Nullzeit

Caspar David Friedrich: Der Winter

Hier jemand, der des Sympathisierens mit linkem oder kommunistischem Gedankengut unverdächtig ist, zum schon diskutierten Thema „Eiszeit oder: Wir Jungdeutschen“ (04.12.2013):
Jede Zeit hat ihr Thema, und jetzt haben wir so eine nihilistische Zeit, da denken die Jugendlichen über Lady Gaga nach. Die Masse war auch früher eher schlicht, aber heute gibt es ja kaum mehr eine intellektuelle Elite, und wenn, kümmert die sich um technische Probleme. Das gesellschaftliche Bewußtsein geht gegen null. (Ole von Beust, CDU, ehemaliger Bürgermeister Hamburgs, in der aktuellen „konkret„)

Kein Wegfall der Geschäftsgrundlage bei der Vorratsdatenspeicherung

Stefan Ansgar Strewe (SPD Sachsen) kommentiert bei Heise das Gutachten des Generalanwalts beim Europäischen Gerichtshof (EuGH) vom 12.12.2014: „Der Wegfall der Geschäftsgrundlage bei der Vorratsdatenspeicherung“.

Man denkt beim flüchtigen Lesen, es gäbe auch bei der SPD vereinzelt Leute, die denken können. Dann aber liest man die Leserkommentare:
Der Gutachter hat gerade nicht empfohlen, die Vorratsdatenspeicherung zu kippen, sondern lediglich eine zeitnahe Überarbeitung der Richtlinie einzufordern, welche die bemängelten Punkte behebt. Dieser Gastkommentar trägt leider nur zur Verdummung der Leser bei, weil diese über wesentliche Tatsachen getäuscht werden.

Man lehnt sich beruhigt zurück: Also doch die SPD, wie man sie kennt.

Kenntnisse empfehlenswert

Stellenanzeige für die Entwicklung von „DeMail“ (via Fefe):
„Protokolle SMTP, IMAP (optional, Kenntnisse empfehlenswert)“

ROTFL. Das gibt bestimmt so etwas wie ELSTER – alles in ~~Java~~ Oracle GlassFish.

Commercial Onion Routing Privacy Service

Eine interessante Frage aus der Tor-Mailingsliste: Offenbar gibt es einen „Anonymisierungs“-Dienst, der von (früheren?) NSA-Mitarbeitern betrieben wird. „It seems a Commercial Onion Routing Privacy Service for US enterprises and Government Agencies.“

Der Dienst heisst NetAbstraction: „NetAbstraction is a Cloud-based service that obscures and varies your network pathways, while protecting your identity and your systems.“

Hinter der Firma steckt eine andere – Cutting Edge CA (vgl. hier).

Nun schauen wir uns Barbara Hunt an, die bei beiden Firmen eine Chefin („Senior Leader“) ist:
My last position in the Intelligence Community (2008-2012) was as Director of Capabilities for Tailored Access Operations at the National Security Agency. As a member of NSA/TAO's senior leadership team, was responsible for end-to-end development and capabilities delivery for a large scale computer network exploitation effort.

Und dann ist da noch Steven W. Bay, Chief Strategist:
Mr. Bay is a retired CIA Senior Operations Officer with 24 years of experience conducting a full range of intelligence operations for the National Clandestine Service, including operational innovation and implementation of telecommunications and information technology programs. Mr. Bay also brings extensive experience in alternate persona research, planning, acquisition, and use.“

Frage in der Mailingliste: „Former spy, experts on COMINT and SIGINT, running an online privacy service?“

Na klar. Denen würde ich sofort meinen Daten anvertrauen. Muahahahaha.

Quantum Computers Animated

Das Original-Video über Quantencomputer ist auf Quantum Jumps. *„Quantum Jumps“ is an exciting collaboration between PHD Comics and the Institute for Quantum Information and Matter (IQIM) at the California Institute of Technology. Using innovative and accessible animations, we will explain the ideas and experimental results at the frontier of Quantum exploration.*

By the way: „Quantenkryptographie ist die Verwendung quantenmechanischer Effekte (besonders bei Quantenkommunikation und Quantencomputern) als Bestandteil kryptographischer Verfahren oder zur Kryptoanalyse. (…) Gegenwärtig können nur extrem eingeschränkte Quantencomputer konstruiert werden. Da es vorstellbar ist, dass in der Zukunft praktisch einsetzbare Quantencomputer gebaut werden können, ist es wichtig, kryptographische Verfahren zu untersuchen, die auch gegen Angreifer mit einem Quantencomputer sicher sind. Dieses Forschungsgebiet wird Post-Quantum-Kryptographie genannt. (…) Der Begriff wurde geprägt, da die ersten asymmetrischen Kryptosysteme auf der Schwierigkeit der Primfaktorzerlegung und der Berechnung diskreter Logarithmen beruhten, zwei Probleme, die theoretisch – bei ausreichend leistungsstarken Quantencomputern – durch den Shor-Algorithmus zu lösen sind. Die Leistungsfähigkeit bisheriger Quantencomputer ist für derartige Berechnungen bei weitem

nicht ausreichend und ein wissenschaftlicher Durchbruch oder Meilenstein kaum vorhersagbar-“

Also keine Panik und keine Hysterie, bitte.

Alices Schwarzer’s Nightmare

„Je ne suis pas un objet sexuel mais une humaine comme tout le monde ce qui prouve qu’elle prend la Pornographie pour son métier et non pas un moyen de divertissement ou une crise d’adolescence.“ (Malena Morgan, Porno-Darstellerin – ich wundere mich natürlich nicht, dass es keine deutsche Wikipedia-Version hierzu gibt.)

Übersetzt: „Ich bin kein Sex-Objekt, sondern ein Mensch wie jeder andere auch, und beweise, dass ich Pornografie für meinen Beruf brauche und weder für mein Privatvergnügen noch um eine Pubertätskrise zu bewältigen.“ Mein Französisch ist schon rostig – hier eine englische Version: „I’m not a sex object but a human like everyone else that proves it takes

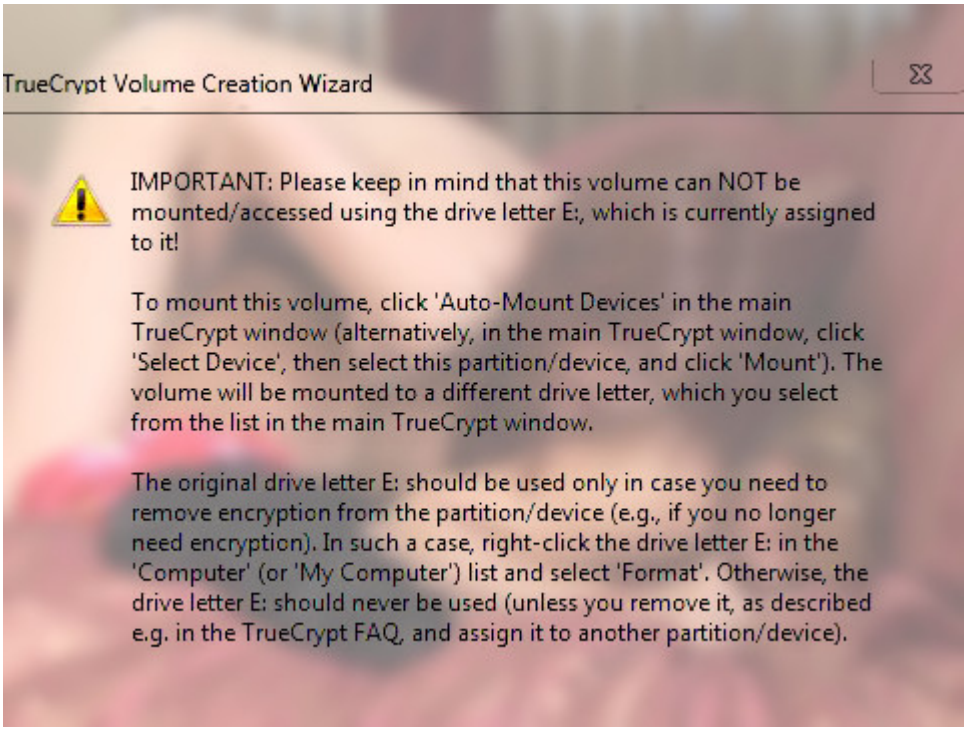
Pornography for his job and not a means of entertainment or a crisis of adolescence.“

Malena Morgan dreht übrigens – bis jetzt und soweit mir bekannt – nur „lesbische“ Pornos (in Anführungszeichen deshalb, weil Porno-Filme, in denen Frauen mit Frauen Sex haben, nicht deshalb schon „lesbisch“ sind – die Zielgruppe sind immer noch und primär heterosexuelle Männer).

Wer jetzt wild herumgoogelt und klickt, weil diese Dame in der Tat ein sehr leckeres Mädel (um mich zu wiederholen) ist, der sei gewarnt: Eine „offizielle“ Website Malena Morgans gibt es nicht, auch wenn mehrere das von sich behaupten. Auch der Twitter-Account ist für mich ein Fake; man muss nur mal ausprobieren, wohin der dort angegebene Link tinyurl.com/TeamMalena in Wahrheit führt (nicht gefährlich). Man lernt pädagogisch wertvoll auch einiges über die kommerziellen Machenschaften der Porno-Industrie.

Foto: Sceenshot eines Youtube-Videos

Terroristisches Material und Pornografie in versteckten Containern glaubhaft abstreiten



Heise: „Die Regierung dürfe Laptops, Kameras und ähnliche Geräte von Reisenden durchsuchen. (…) Richter Korman begründete seine Entscheidung (PDF) damit, dass im 21. Jahrhundert die gefährlichste Schmuggelware oft in Laptops und anderen elektronischen Geräten enthalten sei – zum Beispiel terroristisches Material und Pornografie.“

Im Original: „“In the 21st century, the most dangerous contraband is often contained in laptop computers or other electronic devices, not on paper. This includes terrorist materials and despicable images of child pornography.“

Ein Grund mehr, dass sich auch Nicht-Geeks und Nicht-Nerds mit dem Feature „Hidden Volume“ von Truecrypt beschäftigen.

Deutsche Anleitungen gibt es bei Christian Sickendieck, bei Wikipedia kann man etwas über das „Konzept der glaubhaften Abstreitbarkeit“ (der Begriff ist natürlich Deutsch des Grauens) lesen, und bei bei Truecrypt gibt es alles auch in Englisch. Über die Details hatten wir uns auch schon hier am 15.07.2013 (vgl. auch die Links in den Kommentaren) unterhalten.

Fast ein Quantum Dingsbums

Wieder einmal wird die Panik-Sau durchs Mainstreammedien-Dorf getrieben. Wenn ich bei der NSA wäre, würde ich es auch so machen: So tun, als wäre ich überall schon „drin“, als könne man gar nichts mehr tun, als wären die Geheimdienste übermachtig und allwissen. Genauso kommen die aktuellen Artikel einher: Bürokraten neigen dazu, selbst dem kleinsten Furz eine geheimnisvolle Abkürzung zu geben,

die einschüchtern soll. Heute haben wir die „Quantumtheory“, „Quantumbot“, „Quantumcopper“ und die „NSA-Abteilung Tailored Access Operations (TAO)“. „The Asshole Open“ würde auch passen. Demnächst nennt die NSA *Remote-Access-Software*, die der Zielperson auf DVD per Fahrradkurier zugeschickt wird („Geile-Titten.exe – sofort installieren!) „einstein.exe“ oder so ähnlich.

Und natürlich geistern wieder die „Trojaner“ überall herum (nein, es waren die Griechen, die im Pferd saßen, *nicht* die Trojaner). Es ist alles wie schon bei der so genannten „Online-Durchsuchung“: Wer sich auskennt, lacht sich kaputt, und wer sich nicht auskennt, ist wie gelähmt und macht gar

nichts mehr, weil es angesichts eines solchen übermachtigen Gegners keinen Zweck hat. Genau so ist das gewollt, und alle spielen mit.

Steht in den aktuellen „Enthüllungen“ (es ist alles noch viel schlimmer, als wir uns jemals vorgestellt haben, reloaded und revisited“) überhaupt etwas Neues?

Die TAO kann also angeblich „fast nach Belieben Rechner von Zielpersonen mit Schadsoftware verseuchen.“ Ach ja? Auch Linux? Und wie? Ach so – über das Wie schweigen wir schamhaft, auch wieder wie bei der „Online-Durchsuchung“. Das interessiert ja nicht wirklich. Und „fast“? Fast alle ausser Burks‘ Rechner oder wie?

Früher war es für die NSA noch vergleichsweise mühsam, sich Vollzugriff auf den Computer einer Zielperson zu verschaffen. Sie griff dazu auf eine Methode zurück, die auch Cyberkriminelle und Staatshacker aus anderen Ländern einsetzen: Sie verschickten Spam-E-Mails mit Links, die auf virenverseuchte Webseiten führten.

Normalerweise liest man bei einem derartigen Mupitz nicht weiter. Cookies, Viren, würmer, Trojaner – alles eine Soße.

Wer will da schon die Details wissen. Vielleicht funktioniert die Methode aber bei Spiegel-Online-Redakteuren, sonst würde die das nicht schreiben. Das hatten wir doch schon: „Cipav.exe is an unknown application – install

anyway?“

Lesen wir weiter, wie das Quantum Dingsbums des NSA „funktioniert“:
Eine Quantum-Attacke funktioniert, grob erklärt, folgendermaßen: Zunächst wird der Internet-Traffic an den Punkten, an denen die NSA oder befreundete Dienste darauf Zugriff haben, nach digitalen Lebenszeichen der Zielperson durchkämmt. Das kann eine bestimmte E-Mail-Adresse sein oder etwa ein Webseiten-Cookie.

Schon klar. Cookies. Wer erlaubt die denn, außer Spiegel-Online-Reakteuren? Mein digitales Lebenszeichen ist, wie bekannt, burks@burks.de. Und jetzt?

…kann sich der interessierte NSA-Analyst von dort aus weiterhangeln: Er kann weitere E-Mail-Adressen oder andere Cookies desselben Nutzers suchen, etwa den von Facebook oder Microsofts Hotmail-Dienst.

Ach ja. Dann hangelt mal schön. Es geht munter weiter so:
Statt der eigentlich angeforderten Yahoo-Seite ruft der Browser unbemerkt eine weitere Adresse auf, die von einem NSA-Server stammt.

Also mein Browser macht „unbemerkt“ gar nichts, und wenn doch, würde ich ihn zum Patent anmelden, wegen spontaner Evolution einer künstlichen Intelligenz, die bisher noch unbemerkt in meinen Computern schlummerte. Auch mit dem „Trojaner Olympus“ (beim Zeus, was geben die für Namen?) schwurbeln sie einher, dass es nur so kracht: „Wer sich einmal derartigen Zugang zu einem Computer verschafft hat, kann mit dem infiltrierten Gerät nach Belieben verfahren.“ Wer hätte das gedacht. Aber wie kommt man rein? Spiegel online verweist auf sich selbst: „Die Spione nutzten dazu unter anderem manipulierte Kopien von LinkedIn-Seiten.“

Ach. Das kommt von das. Wer die asozialen Netze, wie die Datenkraken heißen müssten, nutzt, der wird dazu erzogen, die Hosen permanent runterzulassen und alle aktive Inhalte zu erlauben. Ich hingegen erlaube gar nix. Viele Websites sind dann nur noch eingeschränkt lesbar. Quod erat demonstrandum. Webdesigner sind die natürlichen Feinde sicherheitsbewusster Surfer. Und das Geschäftsmodell der Mainstream-Medien, das gar nicht funktionierten würde, verhielten sich die Nutzer so, wie es vernünftig wäre. Bei *Spiegel online* werden munter Cookies gesetzt, man kan sich sogar mit dem Fratzenbuch-Account einloggen, und ohne Javascript bleiben Teile der Website weiß. Das ist so, also würde ein Fleischerladen die Kunden auffordern, vegetarisch zu essen. Pappnasen.

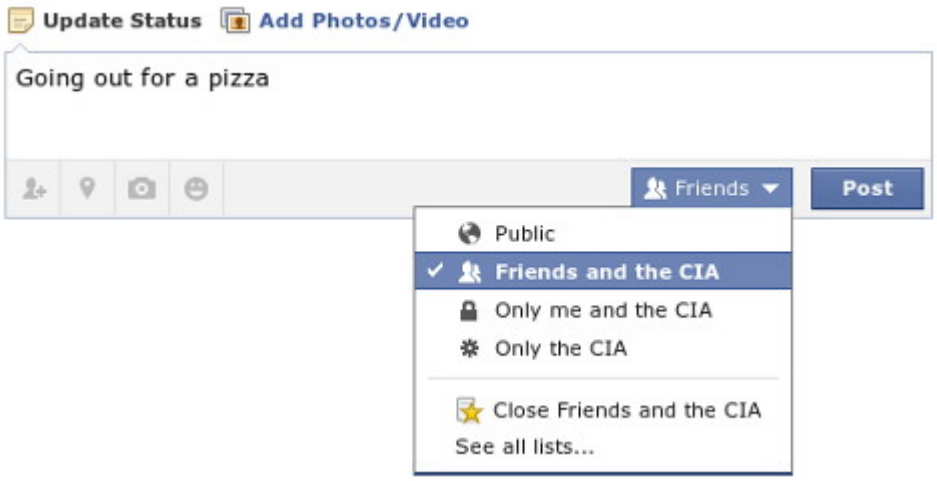
Zu guter Letzt lesen wir ganz unten: „Mitarbeit: Andy Müller-Maguhn“. Dann kann ja nichts mehr schief gehen. Und Tron ist auch ermordet worden, vermutlich von der ~~NDS~~ NSA. Komisch, dass Snowden das nicht erwähnt hat.

No backdoors, never ever

Heise berichtet ausführlich über den Vortrag Roger Dingledines (obwohl von Krempl geschrieben: lesenswert wegen vieler interessanter Details): „Eine Vertreterin des Justizministeriums sei auf die Kernentwickler zugekommen und habe davon gesprochen, dass der US-Kongress Washington das

Recht gegeben habe, ‚alles mit Hintertüren zu versehen'. (…) Der nach Berlin ausgewanderte US-Netzaktivist freute sich besonders, dass Tor insgesamt den ‚Snowden-Sommer' überlebt habe. Er spielte damit auf Enthüllungen des NSA-Whistleblowers an, wonach sich der technische US-Geheimdienst an dem Anonymisierungsnetz bislang mehr oder weniger die Zähne ausgebissen habe."

Das klingt betrüblich



„Mit dem jüngsten Update verlangt die Facebook-App für Android, dass der Anwender ihr weitreichende Rechte einräumt. So will die App nun auch ‚SMS und MMS lesen' und darüber hinaus ‚Kalendertermine sowie vertrauliche Informationen lesen' und ‚ohne das Wissen der Eigentümer Kalendertermine hinzufügen oder ändern und E-Mails an Gäste senden'". (Heise)

Nutzt Facebook! Eine Milliarde ~~Scheißhaus~~Fliegen können nicht irren!