Offline-Durchsuchung

Annalist: “Die Durchsuchung unserer Wohnung hat etwa 15 Stunden gedauert. Genau genommen nicht ganz so lange, denn die eigentliche Durchsuchung fing erst Stunden nach der Stürmung und Andrejs Festnahme an. Mir wurde dazu erklärt, dass nur das BKA durchsuchen könne, und weil aber Meckenheim so weit von Berlin entfernt ist (dort sitzt die Abteilung Linksextremismus des BKA) dauert es, auch bei Tempo 200 und mit Blaulicht über die Autobahn (so der Fahrer mit leuchtenden Augen) eben ein paar Stunden nach Berlin. Die Herren Durchsucher waren wie gesagt eine ganze Weile in unserer Wohnung, und nach und nach haben sie dann auch dies und das erzählt.” [mehr…]

Cockpit

Ähm. Wie fliegt man noch mal gleich einen virtuellen Zeppelin?

Stahlmikado

Credits und Copyright: Alex Friedrich.

Vertrauen ist nicht gut! | Ethno-Zoo

Ein Artikel von mir in der Jungle World über den BND-Skandal – zur Zeit nur in der Printausgabe (kaufen!) Übrigens empfehle ich einen sehr interessanten Artikel von Ivo: “Dänen, Sorben, Rastafaris”. Ich wollte ihm sofort wiedersprechen, aber ich glaube, ich muss mir schon noch genau überlegen, was ich dazu sage….

Zeit des Märtyrertums

“Auf einer islamistischen Website” ist bekanntlich ein Running gag. Danach kommt in deutschen Medien, wie ich mehrfach anzumerken pflegte: Wir haben uns das angesehen, festgestellt, dass unser Publikum angesichts der Inhalte sittlich gefährdet würde, und deshalb verraten wir ihm nicht die Adresse. Wir, die Journaille der Leitmedien, sind hingegen immun gegen Propaganda der islamistischen und sonstigen Art.

Heute wieder Spiegel online: “Im Internet ruft der deutsche Islamist Eric B., der in Pakistan oder Afghanistan vermutet wird, Gesinnungsgenossen zum Dschihad auf. Das Video alarmiert die deutschen Behörden.” Immerhin zeigen sie uns das Filmchen. Aber ich hätte schon gern gewusst, woher sie das geklaut haben (Terroristen führen bekanntlich keine Prozesse wegen Urheberrechtsverletzungen).

Also suchen wir selbst. Es handelt sich um die “für ihre Propagandarolle berüchtigten türkischen Internetseite ‘Zeit

des Märtyrertums'." Ich kann kein Türkisch, weiß also nicht, wonach ich suchen soll. Eine Anfrage bei Google ergibt einen älteren Artikel von Spiegel online – "eine Internetseite, die schon vorher von Sympathisanten der Islamischen Dschihad Union aus Usbekistan (Islamic Jihad Union, IJU) benutzt wurde", findet man da. Über die ominöse Gruppe Islamic Jihad Union hat Telepolis einen ganzen Artikel verfasst: "Terrorgruppe oder Geheimdiensterfindung"? Das ist in der Tat die Frage. Man sollte Craig Murrays Blog dazu aufmerksam lesen.

Nach der Eingabe einiger exakter Zeichenketten habe ich dann die Website Sehadet Vakti gefunden. Bingo. Monitor berichtet: "Eine eigene Website im Internet gibt es nicht, nur einen Eintrag auf der türkischsprachigen Jihadistenseite "Sehadet Vakti". Die ist eine Art Sammelbecken von Hasstiraden und Videos aus dem bewaffneten Kampf."

ZEIT online gibt zu, dass "der Südwestrundfunk und die 'Bild'-Zeitung" über das Video berichtet haben, ist aber nicht in der Lage, die Original-Quellen zu verlinken. [Pfui! Ihr seid doof.] "Das Video ist offenbar erst seit wenigen Stunden im Netz", heisst es beim SWR. Der SWR hat ihre Infos aus den "Sicherheitskreisen", die offenbar die Infos der Journaille aus eigenem Interesse gesteckt haben.

Jetzt habe ich wieder nach einem anstregenden Tag, an dem ich acht Stunden lang junge JournalistInnen in der Internet-Recherche ausgebildet habe, auch noch meine Zeit verschwendet, um das zu tun, was die verdammte Pflicht eines jeden Online-Journalisten gewesen wäre. Gebt mir die Quellen! Gebt mir Links, Links, Links!

Schneller klicken als der eigene Finger

Ein Artikel von mir in der Netzeitung: “Viele Medien haben das ‘Grid’ entdeckt – das so genannte superschnelle Internet. Ist das alles nur ein Hype oder stehen wir wirklich kurz vor dem schnellsten Netz aller Zeiten?”

Wanze trifft Schmiergeld

Ein Artikel von mir auf Telepolis: “Der Bundesnachrichtendienst steht zur Zeit im Fokus der Berichterstattung, weil er vor drei Jahren das Computernetz des [extern] afghanischen Handelsministeriums mit Spionage-Software verwanzt und dessen Korrespondenz belauscht hatte. Die Konzernspitze von Siemens, insbesondere die Kommunikationssparte, war zutiefst korrupt und muss sich derzeit mit einer der größten Schmiergeldaffären in der Geschichte Deutschlands herumschlagen.”

Böhmen in Rixdorf | Ein X für ein S

Wie schon vorgestern verkündet, ziehen wir bald ins so genannte Böhmische Viertel in Rixdorf, in Sichtweite des

idyllischen Richardplatzes. Gestern haben wir die Wohnung ausgemessen, weil wir streichen und Fußböden abschleifen müssen. Unser netter Nachbar hat auch einen Hund, irgendeine Labrador-Mischung. Die beiden Tölchen haben sich gleich angefreundet bzw. Ajax vom Teufelslauch hat dem Nachbarhund dessen Ball geklaut. Der Nachbar war auch mir sympathisch, weil seine Türklingel aus einem alten Atari-Spiel stammt.

Die Umgebung unserer neuen Wohnung ist unglaublich idyllisch. Das Museum im Böhmischen Dorf werde ich mir bald ansehen, vor allem die "Gegenstände, die die Missionare der Herrnhuter aus Missionsgebieten wie Südafrika und Surinam mitbrachten". Wahrscheinlich kann ich zu der kritiklosen Erinnerung an die strenggläubigen Verehrer höherer Wesen noch etwas beitragen. Die Moravier, wie die Herrnhuter auch genannt werden, haben den Osten Nicaraguas missioniert und dort alle gewachsenen indianischen Sozialstrukturen zerstört. Das indirekte Resulat der Mission war, dass die Miskito der Revolution und der Sandinistischen Bewegung feindlich gegenüber standen. [vgl. "Im Land der Miskito" (29.11.2003), "Die Küste der Schildkröten (05.12.2003) sowie meinen Artikel auf Telepolis (25.12.2004) "Kollektiver Wahnsinn".]

Meine neue Stammkneipe (zwei Minuten zu Fuß) habe ich vermutlich auch schon entdeckt. Sie trägt den Namen Café Linus. Vielleicht kann ich die Betreiber überreden, dass S durch ein X zu ersetzen. Der Blogger Schockwellenreiter ist jetzt ein indirekter Nachbar.

Mehr mächtige Spionage-

Werkzeuge, bitte!

Vorgestern hatte ich mich schon über die faktenarmen Textbausteine echauffiert, die jetzt wieder zum Thema "Bundestrojaner" im Umlauf sind. "Der Angriff mittels eines sogenannten [sic] Trojaners", schreibt SPIEGEL Print. Nein. Erstens heißt das Ding "Trojanisches Pferd". Die Trojaner waren das Opfer, nicht die Täter. Und zweitens ist es nicht legitim, jedwede Art von Spionagesoftware jetzt als "Trojaner" zu bezeichnen. Es hat sich bisher auch niemand erkühnt zu behaupten, die Implementierung der Überwachungs-Software sei *online* geschehen.

"Sie schleusen heimlich einen Trojaner in das Computernetzwerk des Ministeriums für Handel und Industrie, eine Spähsoftware, die sich auf den fremden Rechnern einnistet und in aller Stille hilft, den Inhalt der Festplatten nach Deutschland zu schicken. Heimlich schleusen – geht es etwas genauer? Ist das afghanische Netz so unzureichend gesichert, haben es die Deutschen vielleicht selbst aufgebaut, Datenlecks per default inbegriffen? Ich gehe davon aus, dass die Schlapphüte Keylogger und das übliche Zeugs direkt und "händisch" installiert haben – oder denen gleich die ab Werk verwanzten Rechner direkt vor die Nase gestellt haben. Windows, I presume.

Auch im Kongo haben die Geheimdienstler im letzten Jahr Rechner verwanzt, berichtet SPIEGEL Print (28.04.2008, S. 24). "Der Einsatz flog auf, weil einer der BND-Männer das mächtige Spionage-Werkzeug zweckentfremdete, um romantische Postg seiner Partnerin an einen Bundeswehrangehörigen abzufangen." Bruhahaha.

Die Leitung am Hindukusch muss übrigens recht dick sein, wenn man ganze Festplatten (ab 40 Gigabyte aufwärts) verschicken kann, ohne dass die Kisten abrauchen oder alles nur noch in Zeitlupe geschieht. Die "Unterlagen zu diesem Fall wurden

offenbar weitgehend vernichtet". Sehr schön. Also bleibt viel Platz für wildes Herumspekulieren.

"Der Trojaner meldet nach Pullach, dass Farhang eine E-Mail-Adresse des amerikanischen Internet-Anbieters Yahoo nutzt, und das Passwort liefert er gleich mit." Übersetzt heißt das: Ein afghanischer Minister nutzt keine eigenen Server, sondern ein Postfach bei Yahoo. Kann man so blöd sein? Ja, kann man. By the way: "Die Menschenrechtsorganisation Amnesty International hat den US-Unternehmen Microsoft, Google und Yahoo vorgeworfen, bei der Zensur des Internets durch China mitzuwirken." Farhangund seine ganze Behörde haben offenbar vom Internet so viel Ahnung wie Michael Konken vom Bloggen. Und alle schreiben Postkarten. Das ist mittlerweile irgendwie ein Running Gag. Traurig, aber wahr.

Ich gönne ihnen die "Trojaner". Mehr davon, bitte! Gegen die schier unfassbare Naivität, Belehrungsresistenz und Ignoranz der meisten Menschen, die Sicherheit der Daten und der elektronischen Kommunikation betreffend, kann man offenbar erst dann verändern, wenn man ihnen demonstriert, welche Folgen das hat. Ich wette, dass Farhang noch immer Postkarten schreibt, und die betroffene Journalistin auch.

Nachtrag. Die FAZ schreibt: "So sei nicht das persönliche E-Mail-Konto des Ministers, sondern seine Dienst-Mail-Adresse betroffen gewesen, sagte ein BND-Sprecher. Im 'Spiegel'-Bericht sei von einer persönlichen Yahoo-Mail-Adresse des Ministers die Rede. Nach Angaben des BND wird jedoch der gesamt E-Mail-Verkehr des Ministeriums über den amerikanischen Provider Yahoo abgewickelt." Das ist ja noch schlimmer…

Sand im Getriebe

Credits und Copyright: Alex Friedrich.

Weiß am Zug gewinnt

Zum Glück hatte ich die weißen Steine….Wie geht es?

Bundestrojaner beim Afghanen?

Stefan Krempl scheibt bei Heise: “Der Bundesnachrichtendienst (BND) hat Berichten zufolge eine heimliche Online-Durchsuchung beim afghanischen Handels- und Industrieminister Amin Farhang durchgeführt, bei der auch die Kommunikation mit einer Spiegel-Reporterin erfasst worden sein soll.” Ich glaube vorsichtshalber erst einmal gar nichts. Weiter heißt es: “Nach Informationen der Nachrichtenagentur ddp war es dem BND gelungen, mit Hilfe eines Trojaners auf der Festplatte von Farhang ein Spähprogramm zu installieren.” Was sagen die Quellen?

Krempl zitiert sich in typischer Manier selbst: “Die monatelange Observation der Journalistin zwischen Juni und

November 2006, die das Nachrichtenmagazin am Wochenende bekannt machte, war demnach offenbar ein ‘Nebenprodukt’ der Bespitzelung des Spitzenpolitikers”. Das – der zweite Satz des Artikels – suggeriert, als sei die Observation eine “Online-Durchsuchung” gewesen. Das war aber mitnichten so. Hinter dem verlinkten “bekannt geworden verbirgt sich ein Artikel von Spiegel Online, in dem es lediglich heißt: “Der Bundesnachrichtendienst (BND) hat monatelang die E-Mail-Korrespondenz der 42-jährigen SPIEGEL-Reporterin mit dem afghanischen Politiker überwacht und mitgeschnitten.” Das Abhören des Kommunikation hat mit einer Online-Durchsuchung nichts zu tun und ist ein Kinderspiel, wenn die Beteiligten ihre Korrespondenz nicht verschlüsseln. Typisch für das Niveau deutscher Recherche ist auch, dass das “Opfer” Susanne Koelbl meinte, an einen afghanischen Politiker Postkarten schreiben zu müssen und “nicht ahnte”, dass auch andere Leute die lesen wollten – und das natürlich getan haben. Die Kollegin antwortet übrigens nicht auf meine E-Mails zum Thema.

Die Welt online berichtet: “…wurde zum Abschöpfen des E-Mail-Verkehrs zwischen der “Spiegel”-Journalistin Susanne Koelbl und dem Politiker aus Kabul zwischen Juni und November 2006 ein ‘Trojaner’ eingesetzt. Das Spionageprogramm, für dessen Einsatz das Bundesverfassungsgericht unlängst hohe Hürden gesetzt hat, sei auf der Festplatte des Computers des Afghanen installiert worden, hieß es. Dabei seien auch ‘intime Bereiche’ der persönlichen Lebensführung der Journalistin ausgespäht worden.”

Da haben wir’s. Jede Wette, dass der BND den physischen Zugriff auf den Rechner hatte und entweder einen Keylogger oder so etwas sie EnCase® Field Intelligence Model eingesetzt hat. [Vgl. c’t: Der weisse Spion]. Die Stattzeitung für Südbaden erwähnt ein weiteres interessantes Detail: Der heutige afghanische Wirtschaftsminister, ein ehemaliges Mitglied der deutschen Grünen uind “langjährig in Nord-Rhein-Westfalen ansässig,… (…) Die Ausspähung geschah ab 2006 per

Trojaner. Also existiert schon ein funktionsfähiges Modell. Dabei wurde offiziell immer wieder geächzt, wie teuer so was sei und wie schwer zu installieren.” Und genau das ist die Pointe: Der berüchtigte “Bundestrojaner” wird im öffentlichen Diskurs als heimlciher Zugriff über das Internet verstanden. Darum geht es hier aber gar nicht, sondern um ein Spionageprogramm, dass auf der Festplatte installiert worden war. Und so etwas ist gar nicht teuer und auch nicht kompliziert und existiert natürlich schon in verschiedenen Varianten.

Farhang hat das selbst bestätigt, wie die FTD meldet: “Er habe erfahren, dass der BND *seinen Computer im Büro* manipuliert habe. Er gehe davon aus, dass nicht nur einer seiner Computer für wenige Monate überwacht worden sei, wie der BND behaupte. “Ich habe das Vertrauen verloren und nehme an, dass deutsche Agenten alle meine Telefonate und E-Mails noch immer überwachen.” Quod erat deminstrandum.

Falsch im Heise-Bericht ist definitiv: “Im Januar war bekannt geworden, dass der Geheimdienst bereits rund 60 Mal heimlich Zielrechner Verdächtiger im Ausland über das Internet ausgeschnüffelt haben soll”. Soll. Nicht hat. Dass das gar nicht stimmt und auch im damaligen Focus-Artikel falsch war, hat man mir mir telefonisch bestätigt. Es soll damals – durch den BND – nur *eine* “Online-Durchsuchung” gegeben haben, und dafür auch nur eine Quelle. Es ist also gar nichts verifizierbar.

Mass Attack

Die Heise-Meldung von heute habe ich mir genauer angesehen.

“Hunderttausende kürzlich infizierte Webseiten haben mehrere Sicherheitsdienstleister entdeckt. Sie verweisen alle auf einen chinesischen Server und laden von dort ein JavaScript nach, mit dem Besuchern durch das Ausnutzen von Schwachstellen ein Trojaner untergejubelt werden soll. Betroffen sind sogar Seiten von Regierungseinrichtungen wie beispielsweise der Vereinten Nationen (un.org) und von Großbritannien (.gov.uk).”

Die besten Infos gibt es im IIS-Forum. Auch SQL Injection Cheat Sheet könnte in diesem Zusammenhang interessant sein. Es sind nicht nur Windows-Kisten betroffen. Der Angriff modifiziert SQl-Datenbanken. Wer Noscript laufen hat bzw. Javascript per default ausgeschaltet hat (wie ich), dem geschieht nichts. Aber private Surfer haben normalerweise keine Datenbanken hinter sich….

Onanie – jetzt oder nie

ZEIT online über Selbstbefriedigung – sehr schöner Artikel!

Burks kehrt zum Proletariat zurück

Heute haben wir einen Mietvertrag für eine neue Wohnung unterschrieben. Auch den Schlüssel haben wir schon. Nach 26 Jahren in Kreuzberg ziehe ich jetzt in den Stadtteil Neukölln,

ins so genannte Böhmische Viertel in Rixdorf, in Sichtweite des idyllischen Richardplatzes.

“Der Richardplatz ist nach wie vor ein kulturelles Zentrum von Neukölln. Neben zahlreichen Festen stellt der Platz unter anderem durch seine Gastronomie auch einen wichtigen Treffpunkt der Neuköllner Bevölkerung dar. Besonders populär ist der regelmäßig am zweiten Adventswochenende stattfindende traditionell-historische Alt-Rixdorfer Weihnachtsmarkt. Zudem befinden sich dort noch heute alte Gewerbe, wie eine Schmiede und ein Kutschenverleih. Das Fuhrunternehmen Schöne existiert seit 1894. Seit 1910 liegt das Unternehmen am Richardplatz 18. Die Kutschen und Fuhrwerke können noch heute besichtigt werden. Viele Neuköllner schätzen den verkehrsberuhigten Platz vor allem aufgrund seiner Ursprünglichkeit und ruhigen, dörflichen Atmosphäre. Viele der Bauwerke um den Richardplatz stehen heute unter Denkmalschutz und veranschaulichen teilweise noch immer den ursprünglichen Charakter des damaligen böhmischen Dorfes.”

Man glaubt es kaum, wenn man durch die kleinen Straßen wie die Kirchstraße oder den Wantzlikpfad spaziert, dass man in einer Großstadt lebt und in zwei Minuten zu Fuß auf der quirligen Karl-Marx-Straße einkaufen kann. Niedlich ist auch der Böhmische Platz. Auf dem Karl-Marx-Platz ist sogar ein Wochenmarkt. Natürlich ist das Milieu anders als in Kreuzberg, die Preise niedriger und die Läden nicht so schnieke. In Neukölln leben das Proletariat und das so genannte Prekariat, arabische Großfamlilien und der untere türkische Mittelstand. Hier gibt es noch die stilsichere Berliner Eckkneipe, die in Kreuzberg schon fast ausgestorben ist. Dafür ist die Kneipenkultur unterentwickelt. Aber mit dem Fahrrad bin ich ohnehin in 15 Minuten im Görlitzer Park.

Wir haben ein Schnappchen gemacht: Unsere neue Wohnung ist genau so groß wie die jetzige, dafür hat sie einen Balkon, ein zweites Bad, ist hell, liegt in einer verkehrsberuhigten Straße und kostet, weil das Haus außen und das Treppenhaus

nicht renoviert sind, sage und schreibe 250 Euro weniger. Ich kann es noch kaum glauben. Den Grundriss habe ich gleich – einigermaßen maßstabsgerecht – in Second Life nachgebaut. Wer unser neues Zuhause virtuell besichtigen will, kann das noch einige Tage tun in Chokki 18,121,401.

Stasi 2.0, reloaded

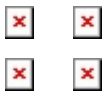
Heise.de unter dem Titel: "Schäuble und die Online-Durchsuchung: "heimliches Betreten der Wohnung" grundgesetzkonform?": "Unionspolitiker sind dagegen der Ansicht, das "heimliches Betreten" genannte Vorgehen zur Installation des Bundestrojaners vor Ort sei keine Wohnungsdurchsuchung und daher grundgesetzkonform."

Die lesen Gesetze und Urteile gar nicht mehr – nach dem Prinzip "legal, illegal, scheißegal". Aus dem Urteil des BVerfG vom 27.02.2008, Randnummer 193: "Darüber hinaus kann eine staatliche Maßnahme, die mit dem heimlichen technischen Zugriff auf ein informationstechnisches System im Zusammenhang steht, an Art. 13 Abs. 1 GG zu messen sein, so beispielsweise, wenn und soweit Mitarbeiter der Ermittlungsbehörde in eine als Wohnung geschützte Räumlichkeit eindringen, um ein dort befindliches informationstechnisches System physisch zu manipulieren. Ein weiterer Anwendungsfall des Art. 13 Abs. 1 GG ist die Infiltration eines informationstechnischen Systems, das sich in einer Wohnung befindet, um mit Hilfe dessen bestimmte Vorgänge innerhalb der Wohnung zu überwachen, etwa indem die an das System angeschlossenen Peripheriegeräte wie ein Mikrofon oder eine Kamera dazu genutzt werden."

Nur zur Erinnerung die Passage im Grundgesetz, Artikel 13, Absatz 1 und 2: "Die Wohnung ist unverletzlich. Durchsuchungen

dürfen nur durch den Richter, bei Gefahr im Verzuge auch durch die in den Gesetzen vorgesehenen anderen Organe angeordnet und nur in der dort vorgeschriebenen Form durchgeführt werden.”

Moments in Second Life



Ja, immer noch viel zu tun. Und heute abend gibt es eine Überraschung. Heute früh jedoch das Übliche, das die wohlwollenden Leserinnen und geneigten Leser sich gähnend abwenden lässt: Cyberhuren im Red-Light-District, zwei Mädels (aber wer weiß das schon genau?) vergnügen sich in einem Zeppelin. Unten: Ich baue gerade alles um. Gegenüber von meinem virtuellen Büro entsteht ein Space-Center mit zweistufigem “Aufzug” (Teleport) direkt in die Weltraumstation. Ich bastele noch an den Details. Es wird eine Weile dauern.

Schon wieder was gewonnen

“Re: Dein Preisgeld
BestÃ€tigungs-E-Mail-Ticket-Nummer: SP338-634
Lotterie Euro / Internationalen E-Mail-Programm Gewinnspiele Dies ist zu informieren, dass Sie Ihre E-Mail-Adresse beigefÃŒgt Zu einem Ticket-Nummer (SP338-634) gewann den Preis Sum Von â¬750.000,00 (Sieben hundertfÃŒnfzigtausend nur) Gewinnspiel in einer E-Mail-Programm am 11. April. 2008. Um

deinen oben angegebenen Preis von â¬750,000.00 zu behaupten, mit dem zugewiesenen verarbeitenvertreter MR.THOMAS SANCHEZ bitte in Verbindung treten. (…) Denken Sie daran, dass alle gewinnen mÃŒssen behauptet, nicht spÃ€ter als 12. Mai. 2008."

Undsoweiter. Super. Eine dreiviertel Million gewonnen. Hole ich gleich in bar ab – in kleinen Scheinen. Man muss dazusagen, dass manche "Newsletter" von Werbefuzzies bei mir, das Layout betreffend, auch nicht besser aussehen.

Auch in Nepal gewinnen die Guten

Tagesschau.de: "Politischer Wechsel nach 240 Jahren Monarchie. Nach über 240 Jahren Monarchie steht Nepal vor einem politischen Wechsel. Ausgerechnet die früheren Untergrundrebellen, die Maoisten, sind die Gewinner der Wahl zur verfassungsgebenden Versammlung. Für eine absolute Mehrheit reicht es aber offenbar nicht."

USA-Vorwahlen

Alle Zahlen zu den Delegiertenwahlen der Demokraten in den USA findet man auf der Website RealClearPolitics – 2008 Elections.