Jetzt schnattert sie wieder…

Nein, Spiegel Offline, auch wenn ihr euch Mühe gebt, die Ente wiederzubeleben: Es gibt *keine* Online-Durchsuchung, auch wenn ihr die „landläufig“ so nennt. Das bayerische Landeskriminalamt hat nach der Methode „legal, illegal, scheissegal“ einem Bürger den Laptop weggenommen und dann eine Spionage-Software installiert.

„Denn der Kaufmann aus Bayern trug nach jener Kontrolle ein wenig mehr im Gepäck als vorher. Auf seinem Rechner hatte das bayerische Landeskriminalamt (LKA) eine Spionage-Software versteckt. Das heimlich am Flughafen installierte Programm sicherte der Polizei weitreichenden Zugriff auf den Laptop. Sobald sich das Gerät ins Internet einwählte, übermittelte es alle 30 Sekunden ein Foto des Bildschirms zu den Ermittlern – gut 60.000 in drei Monaten.“

Ein Keylogger also. Wie das? War der Rechner passwortgesichert? War er nicht mit Truecrpyt verschlüsselt? Konnte man mit admin-Rechten von externen Laufwerken einfach so booten? Wie haben die das also gemacht? *Das will ich wissen und das zu beschreiben wäre Journalismus, Kollege Steffen Winter und nicht so eine gequirlte Gerüchte-Scheiße wie in dem linkfreien Artikel!*

„Im 30-Sekunden-Takt schickte es Fotos der Skype-Oberfläche und des Internet-Browsers an die Ermittler.“ Ach – es geht also nur um Skype? „Wenn das Programm der eigenen Leistungsbeschreibung gefolgt ist, hat es sich dort inzwischen selbst zerstört.“ Und wie heisst das Programm? So eins will ich auch – eine Software, die sich selbst vernichtet! Wieso ist Bill Gates da noch nicht drauf gekommen, so etwas zu erfinden?

Boykottiert de-mail!

Der Bundestag, hat wie zu erwarten war, das De-Mail-Gesetz verabschiedet.

Auf datenspeicherung.de kann man detailliert nachlesen, warum man diesen Unfug auf jeden Fall boykottieren sollte – hier nur wenige Zitate:

„Aufgrund der Architektur von De-Mail fließen alle Daten und Kontakte auf die Person rückführbar an einer zentralen Stelle zusammen;.. (…) Die hinterlegten persönlichen Daten des Nutzers sind für eine Vielzahl von Sicherheitsbehörden und Geheimdiensten ohne richterliche Anordnung anforderbar (§ 113 TKG), die Identität hinter einer De-Mail-Adresse ist für über 1.000 Behörden in einem Onlineverfahren abrufbar (§ 112 TKG (…) Eine Vorratsspeicherung der Verbindungsdaten jeder De-Mail (vgl. § 100 TKG) schließt der Gesetzentwurf nicht aus. Kennung und Passwort zu einem De-Mail-Postfach sind auf Anforderung einer Strafverfolgungsbehörde, einer Polizeibehörde, des Bundesamts für Verfassungsschutz, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes ohne richterliche Anordnung herauszugeben (§ 113 TKG). (…)“

Sicherheitslücken auf Social

Network Portalen

Socialnetworksecurity.org ist ein Blog, das Sicherheitslücken auf Social Network Portalen aufdeckt. (Quelle: Heise)

Hurra, wir sind Zensur-Weltmeister!

Durch ein Posting im Heise-Forum wurde ich auf diesen schon etwa älteren Artikel von SpOff aufmerksam: „Wie die Deutschen Zensur-Vizeweltmeister wurden".

„Sperren, löschen, Personen identifizieren: Google macht jetzt erstmals öffentlich, welche Staaten solche Anfragen stellen. Bei der Entfernung von Videos, Blogeinträgen und Suchtreffern landet Deutschland auf Platz zwei hinter Brasilien – die Gründe sind überraschend banal."

Wieso überraschend? Dass google.de die Deutschen zensiert – ohne zu verraten, was warum zensiert wird -, sollte bekannt sein. Da der Deutsche an sich sich aber gegen derartige Maßnahmen nicht wehrt (wir sind ja keine Tunesier oder Ägypter!), benutzten die Surfer hierzulande brav google.de statt google.com; viiele Journalisten scheitern in meinen Seminaren schon daran, google.com überhaupt aufzurufen.

„Auch Google hat die Listen der BPjM über jugendgefährdende Inhalte implementiert. Die gegen Videoinhalte gerichteten Anfragen bezögen sich nicht auf Copyright-Verstöße, wie man vermuten könnte, sagt der Konzernsprecher – sondern auf Probleme wie Verleumdungen, illegale Inhalte, Verstöße gegen Geschäftsbedingungen, auf die Google einfach aufmerksam

gemacht werde. Copyright-Fragen würden in der Regel direkt mit den Rechteinhabern geklärt. Ihnen stehe mit Content ID außerdem ein System zur Verfügung, direkt über YouTube ihre Rechte geltend zu machen. Nach dem Verständnis vieler in den USA ist Deutschland trotzdem ein Land, in dem das Internet zensiert wird – sie verstehen jede Form des Eingriffes in Inhalte als Zensur".

Nach meinen Verständnis übrigens auch, Spiegel offline! Dass es auch in Deutschland Leute gibt – zugegeben: wenige! -, die Zensur ablehnen, könntet ihr ruhig erwähnen.

Noch ein Satz im zitierten Posting ist bemerkenswert: „Gefiltert werden übrigens auch manche Webseiten über ‚Killerspiele' sowie alle Seiten die die BPJM als 'schwer jugendgefährdend' ansieht – selbstverständlich auch für volljährige User. Eine einfache Suche nach ‚BJPM-Modul' fördert ebenfalls sehr aufschlussreiches zutage."

Das erste, was ich nach einer Revolution abschaffen würde, wären die Firma jugendschutz.net und diese unsägliche Zensur-Behörde „Bundesprüfstelle für jugendgefährdende Medien" (BPjM). Aber ich glaube, dass wird zu meinen Lebzeiten nicht mehr geschehen, erst in fünfzig Jahren oder so – weder die Linke noch die Grünen fordern, die Internet-Zensur in Deutschland abzuschaffen. Das sagt ja genug über die hiesige politische Kultur aus.

Turnitin? Docoloc? Google!

Ein Artikel von mir in der taz: „Die Doktorarbeit von Guttenberg soll Plagiate enthalten, auf der Website GuttenPlag Wiki werden angebliche Beweise gesammelt. Nur: wie findet man eigentlich Plagiate?"

Truecrypt – technische Frage [gelöst]

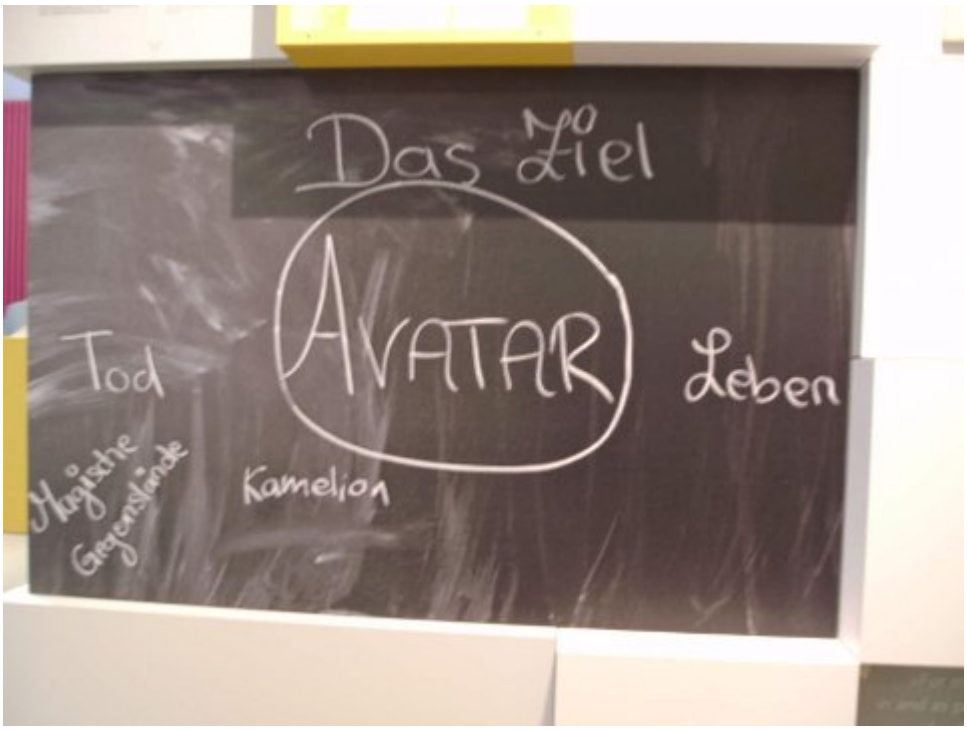
Ich muss die Leserschaft etwas fragen. Ich benutze Truecrypt unter Windows7 (64bit) und unter Ubuntu 10.04. Wenn ich ein Truecrpyt-Laufwerk unter Windows mounte und dann versuche, über mein eigenes Netz per Ubuntu darauf zuzugreifen, werden die gemounteten Truecrypt-Laufwerke des Windows-Rechners nicht angezeigt (alle anderen Dateien kann ich sehen). Was mache ich falsch oder wo ist der Denkfehler?

Das Ziel: Tod, Leben, Avatar


SUPER PONG
SEARS
SELECT GAME
1 2 3 4


VIRTUELLES LEBEN
VIRTUAL LIFE


Die Siedler 2 (1996)



Heute haben ich mir das Computerspielemuseum angeschaut. Wie zu erwarten war, hat das großen Spaß gemacht. Ich musste ununterbrochen schmunzeln.

Hätte man sich jemals vorstellen können, dass ein Commondore, mit dem ich vor einem Vierteljahrhundert gespielt habe, heute hinter Glas in einem Museum zu bewundern ist? Wo ist eigentlich mein Atari, mit dem ich meine ersten Bücher geschrieben habe? (Den habe ich irgendwann verschenkt, ich

Dummkopf.)

Man lernt viel über Kultur – für Schulklassen sollte ein Besuch Pflicht sein. Wie aber archiviert man die Geschichte de 3D-Welten und deren Comic-artigen Anfänge wie Worlds Away aka „Phantasus“? (Das habe ich damals noch mit einem Modem gespielt – kaum zu fassen.)

Wie die Print-Lobby Kinder indoktriniert oder: Der Volkssturm der Holzmedien, revisited

Stefan Niggemeier [via Ulrich Fries und seine Eck.Dose] über den Volkssturm der Holzmedien: „Die Bayerische Staatskanzlei hat im Herbst mit einem Pilotprojekt begonnen, das Grundschülern Medienkompetenz beibringen soll: Sie machen einen Medienführerschein,, den sie in Form einer Urkunde ausgehändigt bekommen. In der Unterrichtseinheit ‚Schau genau hin!, für die dritte und vierte Klasse sollen die Kinder lernen, Nachrichtenwege zu erkennen und zu bewerten.“

Herausgeber der Unterrichtseinheit ist der Verband Bayerischer Zeitungsverleger (VBZV). Was suggeriert also die Broschüre? Wer hätte das gedacht: Blogger sind doof und Zeitungen sind schlau.

Das hatten wir hier schon im Oktober 2009: „Blogger und Journalismus – das war noch nie ein Widerspruch. Ein Blogger muss sich mehr anstrengen, um so viele Leute für sich und seine Meinung zu interessieren, als jemand, der quasi-

verbeamtet in einer (Medien-)Anstalt sitzt, sich auf seinen bezahlten Urlaub verlassen kann und das Usenet nicht von einem Telefonkabel unterscheiden kann."

Aus dem Nachtrag zu Niggemeiers Posting: „Die Staatskanzlei hatte die Initiative für einen Medienführerschein wegen mehrerer Vorkommnisse gestartet. Dazu zählt auch der Amoklauf von Winnenden." Mehrere „Vorkommnisse". Dann kann ja nichts mehr schief gehen. In Deutschland muss jemand Amok laufen, damit jemand auf die Idee kommt, die lieben Kleine zu erziehen, wie man mit Medien umzugehen hat- oder wie darf ich diese „Logik" interpretieren?

By the way: Die Pappnasen von Spiegel Offline schreiben darüber einen linkfreien (!) Artikel. (Oh, eine Ausname – es wird per Link erklärt, was eine „Grundschule" ist!) Ich wüsste schon, wenn ich Diktator Deutschlands wäre, wen ich nicht mehr ohne Medienführerschein das Internet vollschreiben ließe!

Deutscher „Online"-Journalismus at its best

Wirres.net: „in meinem vorherigen artikel habe ich ja behauptet, dass spiegel-online links verkauft und damit das suchmaschinen-ranking der verlinkten site erhöht. frank patalong, leiter des netzwelt-ressorts bei spiegel-online, stellte das in dem artikel den ix kritisierte lediglich als eine ‚weit verbreitete Praxis' in der ‚Blog-Szene' dar, und vergass zu erwähnen, dass es ebenfalls eine weit verbreitete praxis im gesamten internet und insbesondere auch auf webseiten grosser medienhäuser und eben spiegel-online ist. (…) tatsache ist: spiegel-online verkauft links und

kennzeichnet diese nicht wie von suchmaschinen gefordert als bezahlte links.“

Das erklärt natürlich, warum sich die Mainstream- und Holzmedien – aka Spiegel „online“, Focus „online“ und wie sie sich alle nennen mögen – mit irrationaler Beratungsresistenz weigern, Links ausser auf sich selbst zu setzen. Sie würden das erst dann tun, wenn jemand sie dafür bezahlte! Ist schon klar: Wir leben im Kapitalismus und da gibt es eben nichts umsonst. Wo kämen wir denn da hin… Bruhahahaha.

Von Ägypten lernen heisst das Internet abschalten lernen

Futurezone.at: „Im Bundeskanzleramt arbeitet man an einem Projekt, um bei Cyberattacken im EU-Raum Internet und Mobilfunk abschalten zu können.“ (vgl. auch Heise)

War ja klar. Österreich will den Kill-Switch aka „Resetknopf“ wie in Ägypten. Wäre ja noch schöner, wenn die Untertanen einfach kommunizieren könnten, ohne dass die Obrigkeit das erlaubt.

Was mich am meisten wundert, dass ausser dem Bund Deutscher Kriminalbeamter (der immer für den größtmöglichen Unsinn gut ist) das noch niemand in Deutschland gefordert hat. Bosbach, Uhl und Ziercke – übernehmen sie!

Und ewig grüsst der Standort

Heute steht bei Spiegel offline: „Mit Lästereien über die Polizei verriet er sich selbst: Ein 19-Jähriger hatte bei einem Banküberfall 2500 Euro erbeutet und sich dann über die Ermittler lustig gemacht. (…) ‚Das ist doch keine angemessene Polizeiarbeit', schrieb er unter anderem. Die Fahnder ermittelten den Standort des Computers und schnappten den Auszubildenden."

Die Geschichte kam mir gleich bekannt vor. Bingo. Am 18.08.2010 hatten wir das Thema schon einmal.

Damals schrieb SpOff: „Eine Woche nach einem Banküberfall im Bayern hat die Polizei in Hamburg den mutmaßlichen Täter festgenommen. Zum Verhängnis wurde ihm eine E-Mail, in der er hämisch über die Fahnder hergezogen hatte. (…) Nun schrieb der 19-Jährige in Hamburg eine Mail an Zeitungen und Polizei und machte sich über die Fahnder lustig – wohl ohne zu wissen, dass der Standort jedes Computers ermittelt werden kann (…) „Das ist doch keine angemessene Polizeiarbeit", soll es in der Mail vorwurfsvoll geheißen haben."

Natürlich ist es derselbe Mann. Und ich frage mich immer noch, wo der „Standort" einer IP-Adresse ist.

Skype abhören oder wie sich deutsche Richter das E-Mail-

Schreiben vorstellen

Der Beschluss wurde im Auftrag der Staatsanwaltschaft Landshut von den Polizeibehörden vollzogen. Hierzu hat das Bayerische Landeskriminalamt zum Zwecke der Ausleitung der verschlüsselten Telekommunikation auf dem Computer des Beschuldigten [redacted] eine Software aufgebracht, welche über zwei Überwachungsfunktionen verfügt: Die Überwachung und Ausleitung der verschlüsselten Skype-Kommunikation (Voice-over-IP sowie Chat) vor der Ver- bzw. nach der Entschlüsselung sowie das Erstellen von Screenshots der Skype-Software sowie des Internet-Browsers Firefox im Intervall von 30 Sekunden zur Überwachung der über https geführten Telekommunikation. Diese Maßnahmen wurden sodann auch umgesetzt.

Der Beschuldigte wurde von den durchgeführten Telekommunikationsmaßnahmen nicht unterrichtet.

Beschluss des Landgerichts Landshut: „Zwar muss der Beschuldigte um eine E-Mail verfassen zu können, eine Verbindung zu einem Server aufbauen, der ihm die erforderliche Maske zur Verfügung stellt. Der Vorgang des Schreibens der E-Mail findet dann aber ohne Datenaustausch statt, da die einzelnen Buchstaben nicht sofort an den Server weiter übertragen werden. Die E-Mail wird erst dann zum Server und damit in die Außenwelt transportiert, wenn der Beschuldigte den IIVersenden-Button“ betätigt. Hält man sich diese technischen Vorgänge vor Augen, kann nach Auffassung der Kammer – auch im Lichte der Entscheidung des Bundesverfassungsgerichts zur Unzulässigkeit der Online-Durchsuchung (NJW 2008, 822) – beim Schreiben einer E-Mail noch nicht von einern Vorgang der Telekommunikation gesprochen werden.“ (via law blog, mehr dazu bei ijure.org)

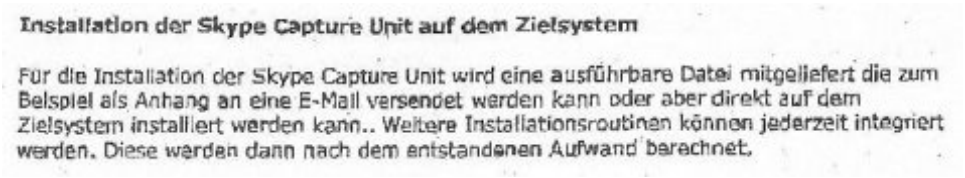
Bruhahahah. Das ist ja wieder ein gefundenes Fressen für unsere Verschwörungstheoretiker zum Thema „Online-Durchsuchung“. Hier geht es aber um Skype (vgl. auch den

Beschluss des LG Landshut dazu.) Der Beschuldigte kommunizierte via Skype und benachrichtigte die Gesprächspartner vorher durch eine SMS.

Frage: Wie kam der so genannte „Trojaner“ (der keiner ist) auf den Rechner des beschuldigten? (Es ging übrigens um die pöhsen Drogen.) Was wäre gewesen, wenn der Beschuldigte *nicht* den Internet-Explorer für Windows, sondern Galeon für Linux benutzt hätte?

Zum Thema habe ich am 09.20.2010 ausführlich gebloggt – „Skype: Heimlich auf den Rechner spielen“:

Udo Vetter scheint vergessen zu haben, dass er zum Thema Skype schon am 17.8.2010 gebloggt hat. Er verwies damals auf den Wikipedia-Eintrag zu Skype, wo man lesen kann, worum es eigentlich geht. Natürlich kann man Skype anhören, aber nicht mit Methoden, die der real gar nicht existierenden „Online-Durchsuchung“ irgendwie ähneln. Man kann also mitnichten, wie Spiegel offline suggiert, einfach so „heimlich“ ein Programm auf fremde Computer „spielen.“ Nein, das kann man nur, wenn man den physikalischen Zugriff hat und Software installieren darf (der Besitzer des Rechner muss also ein DAU sein.)



Installation der Skype Capture Unit auf dem Zielsystem

Für die Installation der Skype Capture Unit wird eine ausführbare Datei mitgeliefert die zum Beispiel als Anhang an eine E-Mail versendet werden kann oder aber direkt auf dem Zielsystem installiert werden kann.. Weitere Installationsroutinen können jederzeit integriert werden. Diese werden dann nach dem entstandenen Aufwand berechnet.

Eine ausführbare Datei, die per E-Mail-Anhang verschickt werden kann? Da lachen ja die Hühner!. Und die installiert das Zielobjekt nichtsahnend? Und der Verdächtige hat auch weder einen Mac noch Linux? Ich zitiere mich selbst vom 27.08.2009:

In der Heise-Meldung von gestern heisst es: „Ein Schweizer Software-Entwickler hat auf seinen Seiten den Quelltext zu einem Programm veröffentlicht, das verschlüsselte Kommunikation über Skype heimlich belauschen kann. Das

Programm ist dazu vorgesehen, als Trojanisches Pferd auf einem PC eingeschmuggelt zu werden. Dort klinkt es sich nach Angaben des Autors in den laufenden Skype-Prozess ein, schneidet die Audio-Daten der Gespräche heimlich mit und lädt sie dann als MP3-Dateien auf einen externen Server.“

Das habe ich mir genauer angesehen. Das Trojanische Pferd ist mitnichten ein „Bundestrojaner“, den es bekanntlich nicht gibt, sondern das Programm Minipanzer: „Minipanzer is a trojan horse that disguises as any kind of file type and when executed on a victims system it collects all sensitive data like account information etc. and sends it to an email address owned by the attacker. It is a one-shot-trojan. It doesn’t install on a target system but only executes its payload and removes itself afterwards.“

Im dazugehörigen Blog heisst es: „The code is simple and straightforward. You have know malware development is no rocket science and if you expect big magic you are at the wrong place.“ Am besten hat mir der Kommentar „Giovannis“ gefallen: „Despite what some people say, Skype has never been secure. It is relatively easy to hack skype accounts, skype does not even check if the same user logs in simultaneusly on different machines and what is worst, the second user can get a copy of all the chats. Skype is good for housewifes that want to chat a bit with their kids, but for confidential conversations the use of strong voice encryption is required. In our company we tested many of them, we now keep with PhoneCrypt from securstar as it proved to be very good, stable, and with an excellent voice quality.“

Ich verweise auf mein hiesiges Posting „“Bayerntrojaner” zum Abhören von Internet-Telefonie?“ sowie auf meinen Artikel in der Netzeitung: „Wenn der Laptop zweimal klingelt“.

Auf law blog gab es einen interessanten Kommentar: „@mark: es geht um einen einfachen Audio-Capture-Client mit Streamingfunktion der sich fernwarten lässt. Der

Programmieraufwand dafür beträgt ca. 20-30 h. Dazu kommt dann die Sonderfunktionalität für Skype die man noch mal mit der gleichen Zeit veranschlagen kann. Dazu noch Tests sowie der Server. Alles in allem ein Projekt, dass sich mit nur einem Mann-Monat stemmen lässt. Selbst bei einem Stundenpreis von vollkommen utopischen 500€ für den Entwickler reden wir hier von Entwicklungskosten im sehr niedrigen 5stelligen Bereich. Bei den Preisen muss die Software nur ein einziges Mal zum Einsatz kommen, damit sie sich für die entwickelnde Firma rechnet. Ich bleibe dabei: hier wird über den Tisch gezogen.“

Nach mal langsam zum Mitschreiben: Man kann nichts heimlich auf fremde Rechner spielen, wenn der Besitzer das nicht will. Kapiert?

Unser Mann in Kairo

Richard Gutjahr bloggt live aus Kairo: „Nachdem heute auch noch Al Jazeera abgeschaltet wurde, habe ich spontan beschlossen, mich nach Kairo durchzuschlagen um selbst dort die Situation zu beobachten (Die Grenze ist von mir aus keine 150 km Luftlinie). Die Übergänge im Süden Israels sind dicht – dafür habe ich noch einen Platz auf dem letzten Flug bekommen, der hier noch rausgeht. Hoffentlich gibt’s keine Probleme bei der Einreise. Ich halte Euch auf dem Laufenden – per Twitter und hier im Blog – so die Netze das zulassen.“ (via Law blog)

Schon dieser Tweet „Internet ist tot. Mobilnetze gibt es drei. Ich wähle… NICHT Vodafone. #prinzipien“ ist schön….

Fidonet in Egypt reloaded [2. Update]

In meinem Taz-Aritikel vom 28.01. lautete der letzte Absatz: „Die ägyptische Opposition greift jetzt zu Mitteln, die schon als technisch veraltet galten. Der Twitter-Nutzer @EgyptFreedomNow gab bekannt, dass das Internet noch per Modem-Einwahl zu einem Provider erreichbar sei, also etwa über ein teures Auslandsgespräch.“ Im Originalmanuskript hieß der Satz übrigens „also etwa per Auslandsgespräch nach Israel“ – das „nach Israel“ wurde von der taz gestrichen.

Vermutlich hat kaum jemand verstanden, was ich damit meinte. Fefe hat jetzt darauf hingewiesen, dass clevere Ägypter angeblich das altehrwürdige Bulletin Board System (BBS) reaktiviert haben, das nur in Deutschland irreführend „Mailboxen“ genannt wird. (Auch Golem hat etwas dazu geschreiben.)

„Actually you can use wi-fi networks/local networks to communicate from one household to another and then if someone can make phone calls abroad/has access to the internet, use it to send packets abroad. Old fidonet software like binkley+/t-mail/hpt/golded/fastecho/frontdoor can be still used. If people in Egypt really need help with this stuff, I guess most of us, fidonet sysops, are ready to help.“

Das Fidonet ist nur eines der BBS-Systeme, die noch existieren, Zone 5 ist für Afrika reserviert. „While the use of FidoNet has dropped dramatically compared with its use up to the mid-1990s, it is still particularly popular in Russia and former USSR. Some BBSes, including those that are now available for users with Internet connections via telnet, also retain their FidoNet netmail and echomail feeds. Some of

FidoNet’s echomail conferences are available via gateways with the Usenet news hierarchy. There are also mail gates for exchanging messages between Internet and FidoNet.“

Vor einem guten Jahrzehnt habe ich auch noch eine Mailbox benutzt (vgl. Sceenshot), und mein vor 16 Jahren erschienenes Buch