```
 CCCCC  H    H    AA    L       I   SSSSS  TTTTTT  I
C       H    H   A  A   L       I  S         TT    I
C       HHHHHH   AAAA   L       I   SSSS     TT    I
C       H    H  A    A  L       I       S    TT    I
 CCCCC  H    H  A    A  LLLLLL  I  SSSSS     TT    I
```

Ausgabe 3

Erlaeuterungen:
DS - Datenschleuder
RC - Redaktion Chalisti
MK - Mik-Magazin
NE - Uebernommen aus einem Netzwerk
FA - Freier Artikel (Autorenangabe am Anfang oder Ende des Artikels)

Die Artikelkennung (CDS1,CMK2,etc) dient zum suchen der Artikel mit Editoren und Textverarbeitungssystemen. Mit der Marke 'NEXT' kann gleich zum naechsten Artikel gesprungen werden.

Editorial

Einige fanden sie gut. Einige fanden sie schlecht. Nun ist sie weg.
Nein. Ich rede nicht von der Chalisti. Gemeint ist das zu Stein gewordene Monument von Hilflosigkeit, Unfreiheit und Teilung einer Welt.
Geboren: 13. August 1961, Gestorben: 9.Novemer 1989. Die Mauer.

Wie viele habe ich in der Nacht vom 9. auf den 10. November vor dem Fernsehen gesehen und konnte kaum glauben was da in Berlin geschah. Am 9.11.1989 wurde nicht die Teilung Deutschlands beendet. Darauf ist weder Deutschland, noch Europa vorbereitet. Es ist viel wichtiger. Man hat angefangen die Teilung der Welt zu beenden. Wenigstens zwischen Ost und West.

Noch ist in dieser Welt viel Konfrontationsdenken angesagt. West vs Ost. Schwarz vs Weiss. Links vs Rechts. CCC vs Post. SW vs RS. Subnet vs Unido. Techniker vs Inhaltler. Die geistige Mauer existiert bei vielen weiter und wird nicht abgerissen. Neues Denken muss ueberall angesagt sein. Nicht einzelne, sondern ganze Gruppen muessen ueber Mauern - auch geistige Mauern - springen.

Die meisten der Leser werden im Jahre 2030 noch Leben. Einige vielleicht auch noch 2050. Auf jeden Fall werden sie von den Zeiten erzaehlen koennen, wo ein Mann in Moskau der Welt die Angst nahm, die Zeit wo die Grossmaechte anfingen die schrecklichsten Waffen die Menschen je ersonnen haben zu vernichten, die Zeit wo die Voelker Europas zusammenwuchsen, die Zeit wo Menschen entdeckten das man die Umwelt und Leben jeglicher Form achten muss, wenn nicht eben diese Umwelt uns vernichten soll. Wir wissen nicht, ob wir in 40 oder 50 Jahren so ueber diese Zeit reden koennen. Solange uns Menschen wie Lobi im Artikel 'Ignoranten' einen Spiegel vorhalten koennen, solange koennen wir nicht sicher sein, dass sich Einsicht ueberall durchsetzt.

Wir haben keine Sicherheit - nicht mal eine hohe Wahrscheinlichkeit - das unsere Welt und unsere Zivilisation weiterbestehen wird. Wir haben aber die Hoffnung. Und das ist schon mehr als in den Jahrzehnten zuvor. Irgendwo hies es mal: 'Was kann der Mensch auf Erden besseres tun, als Mensch zu sein.'. Vielleicht kommt ja wirklich noch die Zeit, dass wir genau das sein koennen:
Menschen.

Das Ende der Mauer in Berlin hat Hoffnung gebracht, viellecht kommen mir daher diese Gedanken gerade in diesen Tagen , obwohl - oder vielleicht gerade weil - wir um das Leben eines Weggefaehrten und Freundes bangen. Den auch uns bleibt nix weiter als die Hoffnung.

Frank Simon

16.11.89

Wir Ignoranten !

Vorwort

Was nun folgt, ist der nackte Wahnsinn der heutigen Zeit.
Was folgt ist keineswegs eine Erzaehlung aus meinem Leben.
Dennoch betrifft das Folgende auch mich zum Teil.
In der Hauptsache aber ist das was folgt EIN Resultat der Beobachtung meiner Umwelt. Eine erschreckende Beobachtung.
Der reale Wahnsinn, von Ignoranz getragen.

Nun geht es los ...

Es wird Zeit, zu sehen wie der mehr oder weniger typische Deutsche seine Umwelt behandelt. Ignorieren wir es einfach,so schlimm kann es nicht werden.

Es ist kaum ein paar Tage her, da fuhr ich mit meinem Buss durch die Innenstadt. Ein Plakat mit der Werbung :"Nicht alles was rot ist, ist Ketchup" ignoriere ich. Das, was fuer den Mann am besten ist, weiss ich selbst am besten ! Ich ignorier es also. (Bilett oder so).
Die alte Dame, die mit einem Fahrschein von anno Domini zu mir kommt, lach ich aus, was gehen mich auch deren Sorgen an ?
Dass mein Wagen 12 Jahre alt ist, und streng genommen eine "Dreck-schleuder" ist ignorier ich. Wer mir mit nem "Kat" kommt, lach ich aus.
Dass ich im Winter zum Skifahren stundenlang fahren muss, wegen des dummen Staus ignorier ich. Stundenlanges anstehen am Skilift geniesse ich als "Ruhepause". Im Herbst gehe ich Bergwandern, aber nicht auf den Berg wo ich Skifahre, der iss ja im Sommer kahl, braun und haesslich.
Dass ich im Sommer mit tausenden von Leuten im gleichen See baade stoert mich schon seit meiner Kindheit nicht. Dass das Gras an den Seen heute laengst nicht mehr nach Grass riecht, sondern nach Kokosoel wiedert mich an. Aber was solls, da fahr ich eben wo anders hin, breite mein Handtuch am Ufer aus, und reibe mich mit Tiroler Nussoel ein. Na klar, wegen der gefaehrlichen Sonnenstrahlung von wegen dem Ozonloch.
Gegen Abend mach ich mit tausend anderen mein Lagerfeuer an der Isar. Das Holz dazu hol ich wie die anderen aus dem umliegenden Gebuesch, es gibt eh genug kaputte Waelder ! Und ausserdem, all die anderen machen es ja genauso.
Dass ich in der Isar seit Jahrzenten schon nicht mehr baden darf braucht mich nicht zu stoeren, das war schon so, seit ich denken kann.

Letztes Wochenende bin ich mal nicht zu einem der ueberlaufenen Seen gefahren, hab da nen Tip von nem Freund bekommen, ganz abgelegen, "den See kennt keiner", so nach dem Motto. Und das hatt ich dann auch davon, die letzten Kilometer zum See waren dann auch Sandstrasse. Sauerei sowas, wende da mehr als 40 faehrst, kannste deinen Wagen waschen lassen.
Wird Zeit, dass die da mal teeren !

Haehae, ein gutes hatte die Sache allerdings. Auf der Sandstrasse sind mir ein paar "gruene" Oekofreaks auf ihren Fahrraedern begegnet. hihi, kurz Gas gegeben, und die Staubwolke war perfekt ! Dachte schon, die bruellen gar nicht mehr.

Der See selber war nicht gerade gastfreundlich, lauter Muecken, Schilf

(hab mir die Fuesse aufgeschnitten) und total lackes Wasser.
Das Auto schnell im Gebusch versteckt, zwecks Hitze, (waere fast in dem sch... Dickicht steckengeblieben) und dann flugs die Autobatterie ausgebaut. Schliesslich braucht die Stereoanlage bei den Liegestuehlen richtig "Saft" ! (Auf die Dauer hilft nur Power ! Hab "Van Halen" aufgelegt, und den Lautstaerkeregeler auf Anschlag gestellt !)
Am Nachmittag hab ich dann gemerkt, dass ich den Traeger Bier fuer mich und meine Frau Daheim vergessen hatte. Mist, und in dieser oeden Wildnis gabs ja nicht mal nen Kiosk ! Schon schwach sowas.
Gegen Abend wurden dann die Muecken all zu laestig, also hab ich hurtig mein Zeug ins Auto gepackt. Musste nur noch schnell meinen Muell im Unterholz verstecken, braucht ja keiner zu wissen, dass ich hier war. Laut Schild wars'n Biotop oder so. Bloedsinn, hab ausser Insekten kein Tier gesehen.
Nur noch schnell gucken, wo die naechste Autobahn laeuft, und dann schnell nach Hause.

Mensch hab ich mich geargert, beim Heimfahren. Hab doch glatt meinen Sperrmuell Daheim vergessen. Hmm, und wohin mit den alten Farbresten vom Malern ? Hatt ich die nicht vor 2 Jahren einfach in die Muelltonne geworfen ? Nee, hab'se vorher im Kloo ausgeleert. Sonst schimpft der Hausmeister wieder, weil der Tonnenraum von Farbresten versaut ist. Einfach ignorieren, den bloeden Tuerken !

Ueberhaupt, fragt mich doch letztens das halbwuechsige tuerkische Freuchtchen (Sohn vom Hausmeister) in der Garage nach 'ner Zigarette. Der soll doch Zuhause in der Tuerkei rauchen, wenn er's sich leisten kann. Alles Arbeitsscheue, diese Tuerken, und dann noch brave deutsche Buerger anschnorren. Das Letzte ist das !

Und stinken tuts bei denen in der Wohnung ! Grauenhaft. Meine Frau hat mir mal erzaehlt, dass es bei denen in der Wohnung aussieht wie bei Hempels unterm Sofa. Ist schon ein schlampiges Volk, diese Auslaender !
Meine Frau war damals zu dem tuerkischen Hausmeister gegangen, weil bei uns ein Hahn tropfte, und dieser faule Gastarbeiter hielt es erst nach 3 Tagen fuer noetig, bei uns vorbeizuschaun. Solange haben wir aber erst gar nicht gewartet, war ja klar dass der nicht kommt. Gleich wie meine Frau von dem Schlamper zurueckkam, hatt sie den Brief an die Hausverwaltung aufgesetzt, mit ner saftigen Beschwerde ueber den Hausmeister natuerlich. Und die haben auch prompt reagiert. Genau als der Tuerke kam um den Hahn zu reparieren, rief uns die Hausverwaltung an, entschuldigte sich, (faselten irgendwas von personellem Notstand) und versprachen, den Auslaender zum naechsten 1. zu kuendigen. Alles Kinkerlitzchen sag ich, fristlos waere die einzig richtige Massnahme, und dann auch gleich das ganze Pack, mit Kind und Kegel dahin zurueckschicken, woher sie gekommen sind !

Na jedenfalls, als der Muselman dann kam, hab ich ihn gleich wieder rausgeworfen, sowas kommt mir doch nicht in die Wohnung. Wer weiss, wenn die Nachbarn mitbekommen haetten, dass ich nen Tuerken reinlass, haette es gleich wieder ein Gerede gegeben. Vonwegen Tuerken-Freund und so.
Nee, das passiert mir nicht !
Mann stelle sich das vor, als ich dem faulen Tuerken dann im Hausgang so richtig die Meinung gesagt habe, wollte er sich auch noch aufregen.
Er, er der Gastarbeiter will mich vor meiner Wohnungstuer, in meinem Land einen krummen Hund und scheiss Deutscher heissen ! Na ja, gesagt hat er es nicht, aber er wollte ! Meine Frau jedenfalls wird bezeugen sie haette es gehoert. Die Anzeige wegen uebler Nachrede hatt er auf alle Faelle bekommen. Waer ja noch schoener. Der soll erstmal richtig blechen, bevor er in die Tuerkei abgeschoben wird ! Fuer was hab ich denn sonst eine Rechtsschutzversicherung ?

Meine Frau und ich haben uns entschieden, in Zukunft fremdlaendische Lokale zu meiden. Der "Grieche" hat uns damals ja einen unzumutbaren

Frass vorgesetzt. Wir gehen, wenn ueberhaupt nur noch zu "Francesco". Das ist zwar auch ein Italiener, aber die Kinder moegen halt so gern die Spaghetti. (ich moecht ja nix sagen, aber das ist ein richtiger Papagello. Wie der sich seine Lizenz fuer die Wirtschaft ergaunert hat wuerd mich auch interessieren. Wahrscheinlich ueber die Maffia.)
Vor 2 Jahren ist sein Lokal abgebrannt, klarer Fall von Schutzgeldern. Ich glaub nicht, dass der das Lokal noch lange hat.
Aber das ist uns wurscht.
Dieses Jahr wollten wir uebrigens nach Jesolo fahren. Das haben wir aber abgesagt, da solls ja auch die Algenpest haben.
Das ist auch wieder typisch fuer diese Auslaender, die lassen das Meer einfach verschmutzen, und muten dann uns Deutschen zu, das wir da reingehen. Jetzt warten wir halt, bis das grosse Schwimmbad bei Jesolo oder so fertig ist. Das ist auch ganz gut so, dann brauchen unsere Kinder nicht immer dieses Salzwasser beim baden verschlucken.
Jetzt bleiben wie dieses Jahr halt in Deutschland, im Urlaub.
Ist auch nicht schlecht, da sparen wir eine Menge Geld.

Das koennen wir naechstes Jahr ganz gut fuer die neuen Moebel gebrauchen. Wir ziehen in eine Sozialwohnung. Das hoert sich zwar schlimm an, ist aber eine Super Sache. Das ist ein Neubau, 105 qm in guestiger Lage, und fuer nur 645,- DM. Ja, ich bin ja nicht bloed, und zahl die Wahnsinnssummen auf dem freien Wohnungsmarkt. Ich verdien ja nicht schlecht, meine Frau arbeitet auch halbtags (schwarz natuerlich), aber bei 1400,- Mark Miete + Nebenkosten koennten wir uns dann nicht mehr 3 Urlaube im Jahr leisten. Ausserdem wollen wir ja unseren Kindern was bieten.
Wir haben damals zur Ueberpruefung vom Sozialamt meine Schwiegeroma fuer ein viertel Jahr zu uns aus dem Altersheim geholt. Mit unseren 2 Kindern, war das dann auch gar kein Problem, dass wir die neue Wohnung bekommen. Aber das viertel Jahr war schon ekelhaft. Immer die alte Person bei uns in der Wohnung, das ist schon eine Belastung. Und stinken tut so ein alter Mensch, das glaubt man gar nicht. Die alten Leut waschen sich ja auch nicht. Aber uns war das nur recht, grad wegen der Frau vom Sozialamt. Natuerlich hab ich die alte Oma nicht gewaschen, meine Frau erst recht nicht. Der hat es ja noch mehr davor geekelt. Wir haben halt recht drauf geschaut, das die Omo schoen in ihrem Zimmer bleibt, das sie nicht so stoert. Sie hat das Zimmer mit unserem Kleinen gehabt, dem hat der Gestank nix ausgemacht, der macht ja selber noch in die Hosen.
Es war eine harte Zeit, aber jetzt ist die Alte ja wieder im Heim. Da ist sie gut aufgehoben und stoert niemanden. Das klingt vieleicht hart, aber so ist die Realitaet. In der heutigen Zeit geht's eben nicht mehr anders, da muessen die alten Leute ins Heim, weil man einfach nicht die Zeit hat sich drum zu kuemmern, und es auch laestig wird.
Besucht haben wir sie seither nicht. Das bringt auch nichts, weil entweder erinnern sich die alten Leute durch den Besuch an fruehere Zeiten, und sie erzaehlen irgend einen alten Schmarrn, meisst aber erkennen sie einem nicht einmahl mehr, oder kriegen den Besuch gar nicht mit. Dann war die ganze Plagerei ja eh umsonst. Schad ums Benzin.
Wir schicken der alten Dame alle Weihnacht einfach eine Glueckwunschkarte, die bekommt sie dann vorgelesen, und freut sich dann genauso.
Ich weiss jetzt gar nicht wann die alte Frau eigentlich Geburtstag hat. Ist auch wurscht, Sie kriegts ja eh nicht mehr mit, und ich glaube die Feiern sind auch ganz nett im Altersheim.
Ab und zu schicken wir auch der betreuenden Schwester im Heim einen 20,- Markschein, dann gibt sie sich ein wenig mehr mit der alten Frau ab, und man muss sich spaeter einmal, am Grab keine Vorwuerfe machen.

Jetzt muss ich erstmal zu meinem grossen Sohn ins Zimmer und ihn beruhigen. Der ist noch ein rechter Weichling. Heute ist sein Hund ueberfahren worden. Der heult jetzt Rotz und Wasser. Jetzt geh ich schnell und sag ihm dass er Morgen einen neuen bekommt. Ich muss mich beeilen, weil in 5 Minuten legt meine Frau "Freitag der 13." in den Video ein. Den Film muss ich unbedingt sehen. Und ein paar Flaschen Bier brauch ich auch noch.

Eigenlich ist die Welt schon grausam, aber mit ein wenig Ignoranz zur rechten Zeit kommt man ganz gut durch. Mann muss sich ja auch nicht ueber alles Gedanken machen, oder ?

Lobi / Peter Lobenstein

[Contrib][Chalisti][03] Wir Ignoranten !

Moeglichkeiten des Umweltschutzes

Vor ein paar Tagen habe ich einen sehr interessanten Vortrag von Professor Prosi (Wirschaftswissenschaftler an der Uni Kiel) ueber Umweltschutz in der Marktwirtschaft gehoert und da ich finde, dass seine Ideen so manches der heutigen Probleme loesen koennten, schreibe ich nun einen kleinen Artikel; vielleicht findet ja der eine oder andere Gefallen an den Ideen.

Im Moment sieht es so aus, als waere unsere Marktwirtschaft alleine nicht in der Lage, die Probleme der Umweltverschmutzung zu loesen. Im Gegenteil, sie verschaerft sie sogar. Massnahmen, die zwar gesamtwirtschaftlich aeusserst schaedlich sind, bringen privatwirtschaftlich Vorteile. An einem Beispiel verdeutlicht: Ein Fischer faengt mehr Fische, als das Meer verkraftet -> der Fischbestand kann sich nicht regenerieren. Fuer die Gemeinschaft ist das katastrophal, denn woher soll man jetzt den Fisch nehmen? Ganz abgesehen von den Folgen fuer die Natur ... Der Fischer hingegen hat privatwirtschaftlich voellig richtig gehandelt. Haette er nur den halben Schwarm gefangen, so haette er befuerchten muessen, dass andere Fischer die restliche Haelfte fangen und er so nur den halben Verdienst haette. Genauso steht es bei der Meeresverschmutzung: "Wozu sollen wir aufhoeren, wenn die anderen weitermachen?" Wir handeln also immer so, wie wir es von anderen befuerchten; auf diese Weise geht die Natur zwangslaeufig zu Grunde. Diesen Teufelskreis der Marktwirtschaft nennt man 'Rationalitaetenfalle'.

Wie kann man nun aus dieser Falle entkommen, wenn man die Marktwirtschaft nicht aufgeben will? Es gibt folgende Loesungen:

- Die Nutzungsrechte (bzw. Verschmutzungsrechte) bleiben kostenlos, der Staat begrenzt aber die Hoechstmenge der Verschmutzung.
  Vorteil: Die Verschmutzung waechst nicht ins Grenzenlose, die Politiker brauchen kaum Erpressungsversuche der Industrie zu befuerchten (teurer Umweltschutz -> Arbeitplatzvernichtung)
  Nachteil: Es besteht kein Anreiz fuer die Industrie (und die Privatleute), die Verschmutzungsmenge zu verringern, wenn man mal von der Verantwortung gegenueber der Natur absieht. Aber wie wirkungsvoll diese Motivation ist, sieht man ja heute.

- Die Nutzungsrechte werden exklusiv zugeteilt. Bsp.: Einem Fischer wird ein Gebiet zugeteilt, in dem nur er fischen darf.
  Vorteil: Der Eigentuemer pflegt 'sein' Stueck Natur, damit er es auch in Zukunft nutzen kann.
  Nachteil: Praktisch wenn ueberhaupt nur schwer zu realisieren.

- Das Recht auf Umweltverschmutzung wird frei handelbar gemacht, kostet also Geld.
  Vorteile:
  Durch die Kosten, die nun fuer die Verschmutzung entstehen, bildet sich ein Anreiz fuer die Firmen, die Verschmutzung zu begrenzen. Der Prozess wird aehnlich wie beim Einsatz von menschlicher Arbeitskraft ablaufen: In den letzten Jahrhunderten wurde der Einsatz menschlicher Arbeitskraefte immer teurer, so dass im Vergleich zum Bruttosozialprodukt deren Einsatz sank. Den gleichen Effekt muesste eine Verteuerung des Einsatzes von Umwelt haben. Im Gegensatz zum jetzigen System (Hoechstmengen) haette dieses Verfahren auch zur Folge, dass 'freiwillig' Geld in die Forschung nach effektiveren Reinigungsverfahren investiert wird. Durch die freie

Handelbarkeit der 'Anrechtsscheine auf Umweltverschmutzung' wuerden sich die Preise der Nachfrage anpassen, die Umweltnutzung wird also umso teurer, je mehr Unternehmen die Umwelt verschmutzen wollen. Ausserdem kann der Staat weiterhin eine Hoechstmenge festlegen, nun aber insgesamt und nicht pro Unternehmen (die Suche nach besseren Reinigungs-Methoden wird also nicht gebremst).

Was haltet Ihr von der dritten Moeglichkeit? Meiner Meinung nach ist sie einfach ideal, sie waere die Loesung unserer Umweltprobleme. Einen Haken hat die Sache allerdings: die Politiker. Leider wird bei uns im Umweltschutz (noch) zuviel Politik gemacht. Die einen wollen lieber Arbeitsplaetze statt Umwelt, die anderen wollen ihre Steinkohle verbrennen und wieder andere wollen die Gewinne der Industrie nicht sinken sehen. Zur Rettung unserer Umwelt muesste eine unabhaengige Behoerde ueber den Handel mit Umweltnutzungsrechten wachen, so wie die Bundesbank ueber den Geldverkehr wacht. Wer kaeme schon auf die Idee, die Politiker das machen zu lassen? Die wuerden doch nur die Geldmenge steigern und damit in kuerzester Zeit eine Inflation verursachen. Warum aber lassen wir die Politiker ueber so etwas wichtiges wie die Umwelt entscheiden? Wir haben nur eine Umwelt, die duerfen wir nicht der Ruecksichtnahme auf parteipolitische Interessen opfern! Wir brauchen also ein unabhaengiges Bundesumweltamt, keine Umweltministerien.

Natuerlich haben wir nicht nur hier in Deutschland umweltpolitische Probleme, in der Dritten Welt sind die Probleme noch viel groesser. Der Bundestag meint, Brasilien durch ein Einfuhrverbot fuer Tropenhoelzer vom Abholzen der Regenwaelder abhalten zu koennen. Diese Massnahme ist zwar eine Moeglichkeit, dass Abholzen unattraktver zu machen, aber das eigentliche Problem beruehrt sie nicht. Warum werden denn die Regenwaelder abgeholzt? Nur aus purer Raffgier? Wieso vernichten die Menschen in Afrika die letzten Waelder? - Es bleibt ihnen gar nichts anderes uebrig, wenn sie nicht verhungern wollen. Um die Umweltprobleme dort zu loesen, muessen wir die wirtschaftliche Entwicklung dort foerdern und bei uns neue Energieformen entwickeln, die dann spaeter in der Dritten Welt genutzt werden koennen.

Es gibt aber noch eine radikale Massnahme: Wenn wir in den Industriestaaten bestimmte Industriezweige wie z.B. die Stahlindustrie stillegten, so koennten die unterentwickelten Laender mit der Stahlproduktion Geld verdienen, anstatt ihre Regenwaelder abzuholzen. Aber wer von uns will schon auf seinen Videorekorder, seinen Zweitcomputer :-) oder den Farbfernseher verzichten? Wie soll man dann das (psychologische) Problem der Arbeitslosigkeit loesen? Ausserdem kommt dann wieder das Motto "Wir handeln so, wie wir es von anderen befuerchten." zum tragen. Woher wollen wir wissen, ob dann nicht die Industrielaender in die entstandene Luecke draengen?
Es gaebe also Loesungsmoeglichkeiten, aber leider hat sich das menschliche Bewusstsein noch nicht so weit entwickelt. Ob das ueberhaupt moeglich ist?

/
/karus (IKARUS@MAFIA)

G10 - Die Gesetze

Ueber das Gesetz hat es bei seiner Einfuehrung bereits erbitterte Debatten gegeben. Das war 1968. Das mit gutem Grund, da sehr gravierende Einschnitte in Grundrechte vorgenommen wurden, die ausserdem weitgehend der richterlichen Ueberpruefung entzogen wurden.

Neu ist im wesentlichen, dass nun neben den trationellen Post-diensten, auch Telekomunikationsdienste von Drittanbietern erfasst werden. Insoweit eine konsequente Anpassung an veraenderte technische und rechtliche Gegebenheiten (teilweise Aufhebung des Postmonopols).

Was bedeutet das fuer die Mailbox? Sie wird gleichbehandelt, wie andere Telekommunikationsmedien. Endlich wird sie vom Gesetzgeber nicht nur zur Kenntnis, sondern sogar ernst genommen! Warum freut sich da keiner??? ;-)

Die Mailbox, ihre Benutzer und Betreiber werden weder besser noch schlechter behandelt, als das bei anderen Kommunikationsmededien der Fall ist. Warum sollte sie auch? Nur weil Ihr davon betroffen seid?? Macht Euch doch nicht laecherlich...

Von daher ist gegen die Einbeziehung von Mailboxen in das "G10" nichts einzuwenden. An dem "G10" als solches gibt es allerdings viel zu noergeln! Das aber schon seit seiner Einfuehrung. Ihr seid mit Eurer Kritik also da, wo andere schon 1968 waren. Vielleicht waren sogar Eure Eltern damals deswegen auf der Strasse...

Und nun werden auch allmaehlich, mit einer Verspaetung von gut 20 Jahren, ein paar Computerkids wach. Naja, besser spaet als gar nicht. Aber wundert Euch nicht, wenn Euch mit dem Schnee von gestern keiner recht ernst nehmen will.

Guten Morgen, Ihr Blitzmerker!!!

Andy

Doch nun endlich der Gesetzestext:

G10
Gesetz zur Beschraenkung des Brief-, Post- und Fernmeldegeheimnisses
Gesetz zu Artikel 10 Grundgesetz
Fassung: BGBl I 1968, 949

G10 @ 1
Fassung: 1989-06-08
(1) Zur Abwehr von drohenden Gefahren fuer die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschliesslich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages oder der im Land Berlin anwesenden Truppen einer der Drei Maechte sind die Verfassungsschutzbehoerden des Bundes und der Laender, das Amt fuer den militaerischen Abschirmdienst und der Bundesnachrichtendienst berechtigt,

dem Brief-, Post- oder Fernmeldegeheimnis unterliegende Sendungen zu oeffnen und einzusehen sowie den Fernmeldeverkehr zu ueberwachen und aufzuzeichnen.

(2) Die Deutsche Bundespost hat der berechtigten Stelle auf Anordnung Auskunft ueber den Postverkehr zu erteilen und Sendungen, die ihr zur Uebermittlung auf dem Postweg anvertraut sind, auszuhaendigen. Die Deutsche Bundespost und jeder andere Betreiber von Fernmeldeanlagen, die fuer den oeffentlichen Verkehr bestimmt sind, haben der berechtigten Stelle auf Anordnung Auskunft ueber den nach Wirksamwerden der Anordnung durchgefuehrten Fernmeldeverkehr zu erteilen, Sendungen, die ihnen zur Uebermittlung auf dem Fernmeldeweg anvertraut sind, auszuhaendigen sowie die Ueberwachung und Aufzeichnung des Fernmeldeverkehrs zu ermoeglichen. Sie haben fuer die Durchfuehrung der vorstehend genannten Anordnungen das erforderliche Personal bereitzuhalten, das gemaess @ 3 Abs. 2 Nr. 1 des Gesetzes ueber die Zusammenarbeit des Bundes und der Laender in Angelegenheiten des Verfassungsschutzes ueberprueft und zum Zugang zu Verschlusssachen des jeweiligen Geheimhaltungsgrades ermaechtigt ist.

G10 @ 2
Fassung: 1978-09-13

(1) Beschraenkungen nach @ 1 duerfen unter den dort bezeichneten Voraussetzungen angeordnet werden, wenn tatsaechliche Anhaltspunkte fuer den Verdacht bestehen, dass jemand
   1. Straftaten des Friedensverrats oder des Hochverrats (@@ 80, 80a, 81, 82 und 83 des Strafgesetzbuches),
   2. Straftaten der Gefaehrdung des demokratischen Rechtsstaates (@ 84, 85, 86, 87, 88, 89 des Strafgesetzbuches, @@ 20 Abs. 1 Nr. 1, 2, 3 und 4 des Vereinsgesetzes),
   3. Straftaten des Landesverrats und der Gefaehrdung der aeusseren Sicherheit (@@ 94, 95, 96, 97a, 97b, 98, 99, 100, 100a des Strafgesetzbuches),
   4. Straftaten gegen die Landesverteidigung (@@ 109e, 109f, 109g des Strafgesetzbuches),
   5. Straftaten gegen die Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantik-Vertrages oder der im Land Berlin anwesenden Truppen einer der Drei Maechte (@@ 87, 89, 94, 95, 96, 98, 99, 100, 109e, 109f, 109g des Strafgesetzbuches in Verbindung mit Artikel 7 des Vierten Strafrechtsaenderungsgesetzes vom 11. Juni 1957 in der Fassung des Achten Strafrechtsaenderungsgesetzes),
   6. Straftaten nach @ 129a des Strafgesetzbuches oder
   7. Straftaten nach @ 47 Abs. 1 Nr. 7 des Auslaendergesetzes

   plant, begeht oder begangen hat.

(2) Eine Anordnung nach Absatz 1 ist nur zulaessig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert waere. Sie darf sich nur gegen den Verdaechtigen oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie fuer den Verdaechtigen bestimmte oder von ihm herruehrende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdaechtige ihren Anschluss benutzt.

G10 @ 3
Fassung: 1968-08-13

(1) Ausser in den Faellen des @ 2 duerfen Beschraenkungen nach @ 1 fuer Post- und Fernmeldeverkehrsbeziehungen angeordnet werden, die der nach @ 5 zustaendige Bundesminister mit Zustimmung des Abgeordnetengremiums gemaess @ 9 bestimmt. Sie sind nur zulaessig zur Sammlung von Nachrichten ueber Sachverhalte, deren Kenntnis notwendig ist, um die Gefahr eines bewaffneten Angriffs auf die Bundesrepublik Deutschland rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen.

(2) Die durch Massnahmen nach Absatz 1 erlangten Kenntnisse und Unterlagen duerfen nicht zum Nachteil von Personen verwendet werden. Dies gilt nicht, wenn gegen die Person eine Beschraenkung nach @ 2 angeordnet

ist oder wenn tatsaechliche Anhaltspunkte fuer den Verdacht bestehen, dass jemand eine der in @ 2 dieses Gesetzes oder eine andere in @ 138 des Strafgesetzbuches genannte Handlung plant, begeht oder begangen hat.

G10 @ 4
Fassung: 1989-06-08
(1) Beschraenkungen nach @ 1 duerfen nur auf Antrag angeordnet werden.
(2) Antragsberechtigt sind im Rahmen ihres Geschaeftsbereichs
    1. in den Faellen des @ 2
       a) das Bundesamt fuer Verfassungsschutz durch seinen Praesidenten oder dessen Stellvertreter,
       b) die Verfassungsschutzbehoerden der Laender durch ihre Leiter oder deren Stellvertreter,
       c) bei Handlungen gegen die Bundeswehr das Amt fuer den militaerischen Abschirmdienst durch seinen Leiter oder dessen Stellvertreter,
       d) bei Handlungen gegen den Bundesnachrichtendienst dieser durch seinen Praesidenten oder dessen Stellvertreter,
    2. in den Faellen des @ 3 der Bundesnachrichtendienst durch seinen Praesidenten oder dessen Stellvertreter.
(3) Der Antrag ist unter Angabe von Art, Umfang und Dauer der beantragten Beschraenkungsmassnahme schriftlich zu stellen und zu begruenden. Der Antragsteller hat darin darzulegen, dass die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert waere.

G10 @ 5
Fassung: 1989-06-08
(1) Zustaendig fuer die Anordnung nach @ 1 ist bei Antraegen der Verfassungsschutzbehoerden der Laender die zustaendige oberste Landesbehoerde, im uebrigen ein vom Bundeskanzler beauftragter Bundesminister.
(2) Die Anordnung ergeht schriftlich; sie ist dem Antragsteller und der Deutschen Bundespost oder dem anderen Betreiber von Fernmeldeanlagen, die fuer den oeffentlichen Verkehr bestimmt sind, mitzuteilen. In ihr sind Art, Umfang und Dauer der Massnahme zu bestimmen und die zur Ueberwachung berechtigte Stelle anzugeben.
(3) Die Anordnung ist auf hoechstens drei Monate zu befristen. Verlaengerungen um jeweils nicht mehr als drei weitere Monate sind auf Antrag zulaessig, soweit die Voraussetzungen der Anordnung fortbestehen.
(4) Das Bundesamt fuer Verfassungsschutz unterrichtet das jeweilige Landesamt fuer Verfassungsschutz ueber die in dessen Bereich getroffenen Beschraenkungsanordnungen. Die Landesaemter fuer Verfassungsschutz teilen dem Bundesamt fuer Verfassungsschutz die ihnen uebertragenen Beschraenkungsmassnahmen mit.
(5) Beschraenkungsmassnahmen sind den Betroffenen nach ihrer Einstellung mitzuteilen, wenn eine Gefaehrdung des Zwecks der Beschraenkung ausgeschlossen werden kann. Laesst sich in diesem Zeitpunkt noch nicht abschliessend beurteilen, ob diese Voraussetzung vorliegt, ist die Mitteilung vorzunehmen, sobald eine Gefaehrdung des Zwecks der Beschraenkung ausgeschlossen werden kann. Einer Mitteilung bedarf es nicht, wenn diese Voraussetzung auch nach fuenf Jahren noch nicht eingetreten ist. Nach der Mitteilung steht den Betroffenen der Rechtsweg offen; @ 9 Abs. 6 findet keine Anwendung.

G10 @ 6
Fassung: 1968-08-13
(1) In den Faellen des @ 2 muss die Anordnung denjenigen bezeichnen, gegen den sich die Beschraenkungsmassnahme richtet.
(2) Soweit sich in diesen Faellen Massnahmen nach @ 1 auf Sendungen beziehen, sind sie nur hinsichtlich solcher Sendungen zulaessig, bei denen Tatsachen vorliegen, aus welchen zu schliessen ist, dass sie von dem, gegen den sich die Anordnung richtet, herruehren oder fuer ihn bestimmt sind.

G10 @ 7
Fassung: 1989-06-08

(1) Die aus der Anordnung sich ergebenden Massnahmen nach @ 1 Abs. 1 sind unter Verantwortung der antragsberechtigten Stelle und unter Aufsicht eines Bediensteten vorzunehmen, der die Befaehigung zum Richteramt hat.
(2) Liegen die Voraussetzungen der Anordnung nicht mehr vor oder sind die sich aus der Anordnung ergebenden Massnahmen nicht mehr erforderlich, so sind sie unverzueglich zu beenden. Die Beendigung ist der Stelle, die die Anordnung getroffen hat, und der Deutschen Bundespost oder dem anderen Betreiber von Fernmeldeanlagen, die fuer den oeffentlichen Verkehr bestimmt sind, mitzuteilen.
(3) Die durch die Massnahmen erlangten Kenntnisse und Unterlagen duerfen nicht zur Erforschung und Verfolgung anderer als der in @ 2 genannten Handlungen benutzt werden, es sei denn, dass sich aus ihnen tatsaechliche Anhaltspunkte ergeben, dass jemand eine andere in @ 138 des Strafgesetzbuches genannte Straftat zu begehen vorhat, begeht oder begangen hat.
(4) Sind die durch die Massnahmen erlangten Unterlagen ueber einen am Post- und Fernmeldeverkehr Beteiligten zu dem in Absatz 3 genannten Zweck nicht mehr erforderlich, so sind sie unter Aufsicht eines der in Absatz 1 genannten Bediensteten zu vernichten. Ueber die Vernichtung ist eine Niederschrift anzufertigen.

G10 @ 8
Fassung: 1968-08-13

(1) Sendungen des Postverkehrs, die zur Oeffnung und Einsichtnahme der berechtigten Stelle ausgehaendigt worden sind, sind unverzueglich dem Postverkehr wieder zuzufuehren. Telegramme duerfen dem Postverkehr nicht entzogen werden. Der zur Einsichtnahme berechtigten Stelle ist eine Abschrift des Telegramms zu uebergeben.
(2) Die Vorschriften der Strafprozessordnung ueber die Beschlagnahme von Sendungen des Postverkehrs bleiben unberuehrt.

G10 @ 9
Fassung: 1978-09-13

(1) Der nach @ 5 Abs. 1 fuer die Anordnung von Beschraenkungsmassnahmen zustaendige Bundesminister unterrichtet in Abstaenden von hoechstens sechs Monaten ein Gremium, das aus fuenf vom Bundestag bestimmten Abgeordneten besteht, ueber die Durchfuehrung dieses Gesetzes.
(2) Der zustaendige Bundesminister unterrichtet monatlich eine Kommission ueber die von ihm angeordneten Beschraenkungsmassnahmen vor deren Vollzug. Bei Gefahr im Verzug kann er den Vollzug der Beschraenkungsmassnahmen auch bereits vor der Unterrichtung der Kommission anordnen. Die Kommission entscheidet von Amts wegen oder auf Grund von Beschwerden ueber die Zulaessigkeit und Notwendigkeit von Beschraenkungsmassnahmen. Anordnungen, die die Kommission fuer unzulaessig oder nicht notwendig erklaert, hat der zustaendige Bundesminister unverzueglich aufzuheben.
(3) Der zustaendige Bundesminister unterrichtet monatlich die Kommission ueber von ihm vorgenommene Mitteilungen an Betroffene (@ 5 Abs. 5) oder ueber die Gruende, die einer Mitteilung entgegenstehen. In den Faellen des @ 5 Abs. 5 Satz 3 unterrichtet er die Kommission spaetestens fuenf Jahre nach Einstellung der Beschraenkungsmassnahmen ueber seine abschliessende Entscheidung. Haelt die Kommission eine Mitteilung fuer geboten, hat der zustaendige Bundesminister diese unverzueglich zu veranlassen.
(4) Die Kommission besteht aus dem Vorsitzenden, der die Befaehigung zum Richteramt besitzen muss, und zwei Beisitzern. Die Mitglieder der Kommission sind in ihrer Amtsfuehrung unabhaengig und Weisungen nicht unterworfen. Sie werden von dem in Absatz 1 genannten Gremium nach Anhoerung der Bundesregierung fuer die Dauer einer Wahlperiode des Bundestages mit der Massgabe bestellt, dass ihre Amtszeit erst mit der Neubestimmung der Mitglieder der Kommission, spaetestens jedoch drei Monate nach Ablauf der Wahlperiode endet. Die Kommission gibt sich eine Geschaeftsordnung, die der Zustimmung des in Absatz 1 genannten Gremiums bedarf. Vor der Zustimmung ist die Bundesregierung zu hoeren.

(5) Durch den Landesgesetzgeber wird die parlamentarische Kontrolle der nach @ 5 Abs.1 fuer die Anordnung von Beschraenkungsmassnahmen zustaendigen obersten Landesbehoerden und die Ueberpruefung der von ihnen angeordneten Beschraenkungsmassnahmen geregelt.
(6) Im uebrigen ist gegen die Anordnung von Beschraenkungsmassnahmen und ihren Vollzug der Rechtsweg nicht zulaessig.

G10 @ 10
Fassung: 1968-08-13
(1) Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird durch dieses Gesetz eingeschraenkt.
(2) Die auf Grund anderer Gesetze zulaessigen Beschraenkungen dieses Grundrechts bleiben unberuehrt.

G10 @ 11
Fassung: 1968-08-13
Die nach diesem Gesetz berechtigten Stellen haben die Leistungen der Deutschen Bundespost abzugelten.

G10 @ 12
Fassung: 1989-06-08
(1) Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird durch dieses Gesetz eingeschraenkt.
(2) Die auf Grund anderer Gesetze zulaessigen Beschraenkungen dieses Grundrechts bleiben unberuehrt.

G10 @ 13
Fassung: 1989-06-08
Die nach diesem Gesetz berechtigten Stellen haben die Leistungen der Deutschen Bundespost oder anderer Betreiber von Fernmeldeanlagen, die fuer den oeffentlichen Verkehr bestimmt sind, abzugelten.

G10 @ 14
Fassung: 1989-06-08
Artikel 2 und 3 dieses Gesetzes mit Ausnahme des Artikels 2 Nr. 2, @ 100a Nr. 1 Buchstaben b und d, gelten nach Massgabe des @ 13 Abs. 1 des Dritten Ueberleitungsgesetzes vom 4. Januar 1952 (Bundesgesetzbl. I S. 1) auch im Land Berlin.

G10 @ 15
Fassung: 1989-06-08
Dieses Gesetz tritt mit Ausnahme des @ 9 Abs. 4, der am Tage nach der Verkuendung in Kraft tritt, am ersten Tag des auf die Verkuendung folgenden dritten Kalendermonats in Kraft.

Das waren jetzt erstmal nur die G10-Gesetze. Jetzt noch die Aenderungen des Gesetzes uebe Fernmeldeanlagen.
Quelle: Bundesgesetzblatt Nr. 25 14.6.1989

@ 1

(4) Jedemann ist berechtigt, Telekommunikationsdienstleistungen fuer andere ueber Fest- und Waehlverbindungen, die von der Deutschen Bundespost TELEKOM bereitgestellt werden, zu erbringen. Dies gilt nicht fuer das Betreiben von Fernmeldeanlangen, soweit es der Vermittlung von Sprache fuer andere dient; dieses Recht steht ausschliesslich dem Bund zu (Telefondienstmonopol).

@ 1a

(1) Betreiber von Fernmeldeanlagen, die Telekommunikationsdienstleistungen gemaess @ 1 Abs.4 fuer andere erbringen, muessen die Aufnahme des Betriebes sowie Aenderungen und Aufgabe desselben innerhalb eines Monats dem Bundesminister fuer Post und Telekommunikation schriftlich anzeigen.

Der Bundesminister fuer Post und Telekommunikation veroeffentlich diese Anzeigen halbjaehrlich in seinem Amtsblatt.

@ 25

Das ausschliessliche Recht des Bundes, einfache Endeinrichtungen des Telefondienstes zu errichten und zu betreiben, bleibt bis zum 1.7.1990 bestehen.

@ 26

Betreiber von Fernmeldeanlagen, die Telekommunikationsdienstleistungen gemaess @ 1 Abs. 4 fuer andere am 1.7.1989 erbringen, muessen den Betrieb bis zum 1.1.1990 beim Bundesminister fuer Post und Telekommunikation schriftlich anzeigen.

G10: Mailboxen unter Kontrolle der Geheimdienste

Die Telekommunikationsanbieter sollen zum verlaengerten Arm von Polizei und Geheimdiensten gemacht werden. Mit der Verabschiedung des Poststrukturgesetzes wurden - von der Oeffentlichkeit kaum bemerkt - die Ueberwachungsmoeglichkeiten durch Polizei und Geheimdienste bei Telekommunikationsdiensten erheblich erweitert.

Zur Abwehr von drohenden Gefahren fuer die freiheitlich demokratische Grundordnung duerfen die Verfassungsschutzbehoerden (VS), der Militaerische Abschirmdienst (MAD) und der Bundesnachrichtendienst (BND) den Telekommunikationsverkehr ueberwachen und in beliebiger Form mit beliebigen Medien aufzeichnen und in beliebiger Form mit beliebigen Medien aufzeichnen (1). Dasselbe duerfen jetzt die Strafverfolgungsbehoerden im strafrechtlicher Ermillungen gem. Par. 100 a und 100 b StPO. Bislang durften der Fernmeldeverkehr nur auf Tontraeger aufgenommen werden.
Damit sind die rechtlichen Voraussetzungen zur Anwendung jeder beliebigen Speicherungs- und Auswertungstechnik von Sprache und Daten durch die Geheimdienste und Strafverfolgungsbehoerden geschaffen worden. Diese Techniken sind fuer die effektivere Ueberwachung digitalisierter Netze, insbesondere der Kommunikation im ISDN fuer die Geheimdienste von besonderem Interesse.

Bestimmte Ueberwachungsmethoden koennen eine neue Qualitaet erreichen. Bereits 1978 hat der Bundesnachrichtendienst einen bestimmten Prozentsatz des Post- und Fernmeldeverkehrs in die DDR mit folgendem Verfahren ueberwacht (2). Es werden regelmaessig computergesteuert Gespraeche mitgeschnitten, in denen bestimmte Begriffe oder Silben enthalten sind. Diese Auswertungen sind nach einem Urteil des BVerfG von 1985 (3) nur verfassungsmaessig, weil es sich gem. $ 3 G 10 um eine strategische Ueberwachung handele, die Sach- und nicht personenbezogen sei.
Die Partner der Gespraeche blieben unbekannt, weil es im Fernsprechverkehr in der Regel technisch nicht moeglich sei, die Gespraechspartner zu identifizieren, wenn sie nicht selbst, was selten genug der Fall sei, sich im Verlauf des Gespraeches ueber ihre Identitaet aeussern (4), so das BVerfG.

Im ISDN ist dies vermutlich nicht mehr der Fall, falls die Geheimdienste ihre Ueberwachungsmassnahmen in den Vermittlungstellen durchfuehren. Zumindest sind ueber das Gespraechsende die Vermittlungsdaten rekonstruierbar. Die Gespraechspartner lassen sich ueber die Verbindungsdaten in den Vermittlungstellen identifizieren. Die strategische Ueberwachung gem. $ 3 G 10 waere im ISDN personenbeziehbar.

Mit den neuen Dienstleistungsangeboten wie TEMEX, Mailboxen, Pressedienste, elektronischen Bestellungen usw. auf der einen Seite und der Speicherung der Verbindungsdaten im Netz selbst durch die Post auf der anderen Seite, entstehen fuer automatisierte Ueberwachungsverfahren ganz neue Moeglichkeiten.

Zudem muss jeder Telekommunikationsanbieter jetzt fuer die Geheimdienste taetig werden. Auf Anordnung des Innenminsters oder der zustaendigen Laenderbehoerden muessen Telekommunikationsanbieter den Geheimdiensten und Strafverfolgungsbehoerden Auskunft ueber den durchgefuehrten Fernmelde- und Datenverkehr

erteilen, Sendungen die ihnen zur Uebermittlung auf Telekommunikationsnetzen anvertraut worden sind, aushaendigen und die Ueberwachung und Aufzeichnung des Telekommunikationsverkehrs ermoeglichen (5).

Fuer die Durchfuehrung muss jeder Telekommunikationsanbieter derartiger Massnahmen Personal bereithalten, dass nach den Bestimmungen des Gesetzes ueber die Zusammenarbeit des Bundes und der Laender in Angelegenheiten des Verfassungsschutzes vom Verfassungschutz ueberprueft ist und zum Zugang zu Verschlussachen des jeweiligen Geheimhaltungsgrades ermaechtigt ist (6). Damit muss jeder Telekommunikationsanbieter (z.B. Mailboxbetreiber) dem Verfassungsschutz mindestens eine Person zu nennen, die vom Verfassungsschutz sicherheitsueberprueft wird und aufgrund dieser Ueberpruefung die Berechtigung zum Zugang zu Verschlussachen hat. Wer derartiges Personal nicht bereitstellt, kann mit einer Geldbusse bis zu 30.000,- DM bestraft werden (7). Jeder Telekommunikationsanbieter ist verpflichtet, dem Verfassungschutz MitarbeiterInnen zu nennen, die dieser im Rahmen einer Sicherheitsueberpruefung ausschnueffeln darf und die fuer die Ueberwachungsmassnahmen der Geheimdienste zur Verfuegung stehen. Bei Anbietern, die Telekommunikationsdienstleistungen alleine oder zu zweit anbieten, kommt dies einer generellen Sicherheitsueberpruefung von Telekommunikationsanbietern durch den Verfassungschutz gleich. Zudem koennen die zustaendigen Stellen natuerlich jederzeit die Ueberwachungsmassnahmen mit eigenen Mitarbeitern durchfuehren.

Nach dieser Aenderung des G 10 muss jeder Telekommunikationsanbieter und jeder Nutzer damit rechnen, dass die Geheimdienste auch rueckwirkend sowohl die Herausgabe von Daten ueber Verbindungen, als auch den Inhalt z.B. von elektronischen Faechern in Mailboxen, verlangen koennen. Massgeblich fuer die rueckwirkende Herausgabe, ist der Zeitpunkt der Anordnung. Sie ergeht schriftlich und ist dem Telekommunikationsanbieter mitzuteilen. Sie sollte sich jeder Betroffene vorlegen lassen. Andernfalls ist weder Herausgabe noch Ueberwachung zulaessig. Weiterhin muss jeder Telekommunikationsanbieter Ueberwachungsmassnahmen fuer die Zukunft bei Vorliegen einer Anordnung dulden. Diese ist auf hoechstens drei Monate befristet und darf jeweils nur um drei Monate verlaengert werden, falls die Vorraussetzungen der Anordnung fortbestehen.

Die vom Gesetz intendierten Ueberwachungsmassnahmen richten sich dabei nicht primaer gegen den Telekommunikationsanbieter, sondern gegen die Nutzer der Telekommunikationsdienste. Der Telekommunikationsanbieter wird im Falle von Ueberwachungsmaanahmen einer besonderen Schweigepflicht unterworfen (8). Teilt er einem anderen die Tatsache der Ueberwachung mit, so kann mit Freiheitstrafe bis zu zwei Jahren bestraft werden.

Ein zynischer Wermutstropfen: Die Geheimdienste bezahlen alle Leistungen, die fuer sie im Rahmen von

8 $ 10 Abs.1 G 10.
9 $ 13 G 10.

Jochen Riess / Institut fuer Informatios- und Kommunikationsoekologie
Uni Bremen/Prof. Kubiczek

G10: Mik Magazin schreibt dazu ...

Hamburg/Bonn (emp/mik) - Die im Zuge der Postreform auf private Betreiber von Vermittlungseinrichtungen ausgedehnten Beschraenkungen des Fernmeldegeheimnisses gelten nach Auskunft des Bundespostministeriums nicht fuer Mailbox-Systeme. Dies teilte das Ministerium der Oberpostdirektion Bremen auf Anfrage mit, nachdem verschiedene Bremer Mailbox-Betreiber ihr zustaendiges Fernmeldeamt ueber die neue Rechtslage befragt hatten. Nach der Neufassung des Gesetzes zur Beschraenkung des Fernmeldegeheimnisses, die seit dem 1. Juli 1989 gilt, ist nicht nur die Deutsche Bundespost, sondern auch jeder andere Betreiber oeffentlicher Vermittlungseinrichtungen gesetzlich verpflichtet, den staatlichen Sicherheitsorganen die ihm anvertrauten Brief-sendungen auszuhaendigen und die Ueberwachung des Fernmelde-verkehrs zuzulassen. Private Kommunikations-Dienstleister muessen zudem Mitarbeiter benennen, die mit den Sicherheits-behoerden zusammenarbeiten und Verschlusssachen auf Anordnungen aushaendigen.

Nach allem was man weiss, so das Ministerium, fallen die Mailboxen nicht unter die Anmeldepflicht. Man habe weder Formulare fuer Mailboxen, noch gehe man davon aus, dass man die vielen Mailbox-Systeme ueberhaupt verwaltungstechnisch registrieren koennte - selbst wenn man wollte. Ferner sei der Begriff "Fernmeldeanlage" im Gesetz technisch und formal zu verstehen. Gemeint seien Vermittlungseinrichtungen. Zwar fallen Mailboxen auch unter Fernmeldeanlagen oder Fernmeldedienstleistungen, nicht aber unter den technischen Begriff der "Vermittlungseinrichtung". Dies gelte auch fuer vernetzte Mailbox-Systeme. Sollte sich an dieser Interpretation etwas aendern, werde das Ministerium darueber umgehend informieren.

Nach dem Gesetz droht dem Betreiber einer Vermittlungsein-richtung ein Bussgeld bis zu dreissigtausend Mark, wenn er sich weigert, mit Geheimdiensten und staatlichen Sicherheitsbehoerden zusammenzuarbeiten. Als Weigerung wird angesehen, wenn Sendungen nicht aushaendigt oder das Ueberwachen%Uedes Fernmeldeverkehrs nicht ermoeglicht werden. Gleiches gilt fuer Betreiber, die keine Mit-arbeiter stellen, die mit staatlichen Geheimdiensten zusammenarbeiten. Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe werden dem angedroht, der eine angeordnete Ueberwachung des Fernmeldeverkehrs anderen mitteilt.

Als "masslose Selbstueberschaetzung" bezeichneten Bonner Rechtsexperten die Auffassung politischer Beobachter, die in der Neufassung des Gesetzes einen gezielten Seitenhieb auf den E-Mail-Bereich oder gar einzelne Nutzergruppen wie Umweltschuetzer oder linke Gruppen sehen wollen. In diesem Sinne hatte die Illustrierte Stern das Thema aufgegriffen. Das Blatt sprach von "Spitzeln in der Mailbox" und einer Reaktion bundesdeutscher Geheimdienste, denen die Mailbox-Szene "schon lange ein Dorn im Auge" gewesen sei. Wie das Bundespostministerium auf Anfrage erklaerte, sei die Ausdehnung der Ueberwachungsmoeglichkeiten auf

private Betreiber eine Konsequenz der Poststrukturreform. Ohne die Neufassung waere eine Situation entstanden, bei der nur die Deutsche Bundespost zur Offenlegung der Daten gegenueber Geheimdiensten verpflichtet waere.

In einer von der GeoNet Mailbox Services GmbH Haunetal in Auftrag gegebenen Kurz-Analyse der neuen Bestimmungen heisst es unter anderem, dass die Verfasser des Gesetzes irrigerweise davon ausgegangen seien, dass kuenftig nur grosse, institutionalisierte Anbieter in Konkurrenz zur Bundespost treten wuerden. Dies beweise insbesondere die Tatsache, "dass das Nichtvorhalten ueberprueften Personals mit einer nicht unbetraechtlichen Geldstrafe bedroht wird". Darueber hinaus sei es kaum gelungen, eine geeignete Definition anzubieten, welche tatsaechlich alle Dienstleitungstypen abdecke. So koenne man das Gesetz auch so auslegen, dass Stand-Alone-Mailbox-Systeme nicht unter diese Vorschrift subsumiert werden koennen. Dies alles aendere jedoch nichts daran, dass die E-Mail-Branche mit diesem Gesetz zu leben habe. Im Sinne der Benutzer sei es deshalb sinnvoll, Nachrichten kuenftig verschluesselt abzuspeichern, wodurch sich auch eine Reihe datenschutzrechtlicher Probleme elegant loesen liessen.

E-Mail-Press/MIK Magazin

[Contrib][Chalisti][03] G10: Mik Magazin schreibt dazu ...

Parteien und Behoerden zum G-10

Im Zuge der Aenderung der Neustrukturierung des Post- und Fernmeldewesens wurde auch der Artikel 10 des Grundgesetzes und der 100a, 100b der Strafprozessordnung geaendert.

Hier ein Auszug aus dem Bericht des Bundestagsausschusses fuer das Post- und Fernmeldewesen (Bundestagsdrucksache 11/4316):

"Die stuermische technologische Entwicklung mit einem immer schneller wachsenden Bedarf an innovativen Kommunikationsdiensten macht eine Reform des Post- und Fernmeldewesens und der Deutschen Bundespost erforderlich, weil die heutigen institutionellen und ordnungspolitischen Strukturen den zukuenftigen Anforderungen nicht mehr in ausreichendem Masse gerecht werden."

So hat denn der Ausschuss maechtig viel gearbeitet. Die GRUENEN, die gegen eine Aenderung sind, haben sich an den Beratungen nicht beteiligt. Die SPD hat zwar "grundsaetzlich einen Regelungsbedarf anerkannt, jedoch erhebliche Bedenken gegen das vorliegende Gesetzgebungsverfahren, in dem ohne gruendliche Parlamentarische Beratung die gesetzliche zulaessigen Ueberwachungsmassnahmen auf jegliche Art des Fernmeldeverkehrs erstreckt werden sollen, geltend gemacht." (Auszug aus einem Schreiben von Arne Boernsen, Obmann der SPD).
Die Regierungskoalitionsparteien meinen, dass der Satelitenfunk, das geplante europaische Mobilfunknetz D und andere Mobile Funknetze, in denen neben der Deutschen Bundespost weitere Private Anbieter zugelassen sind "sich generell zur konspirativen Kommunkation von Personen, die Straftaten nach 2 Abs.1 des G-10 planen behen oder begangen haben" eignet. (Bundestagsdrucksache 11/4316 S. 79)

Herausgekommen ist u.a. folgendes:
"Das Gesetz zur Beschraenkung des Brief-, Post- und Fernmeldegeheimnisses wird wie folgt geaendert:

Artikel 1 1 Abs. 2
Die Deutsche Bundespost hat der berechtigten Stelle auf Anordnung Auskunft ueber den Postverkehr zu erteilen und Sendungen, die ihr zur Uebermittlung auf dem Postwege anvertraut sind, auszuhaendigen. Die Deutsche Bundespost und jeder andere Betreiber von Fernmeldeanlagen, die fuer den oeffentlichen Verkehr bestimmt sind, haben der berechtigten Stelle auf Anordnung Auskunft ueber den nach Wirksamwerden der Anordnung durchgefuehrten Fernmeldeverkehr zu erteilen, Sendungen, die ihnen zur Uebermittlung auf dem Fernmeldeweg anvertraut sind, auszuhaendigen sowie die Ueberwachung und Aufzeichnung des Fernmeldeverkehrs zu ermoeglichen. Sie haben fuer die Durchfuehrung der vorstehend genannten Anordnungen das erforderliche Personal bereituzhalten, das gemaess @3 Abs.2 Nr.1 des Gesetzes ueber die Zusammenarbeit des Bundes und der Laender in Angelegenheiten des Verfassungsschutzes ueberprueft und zum Zugang zu Verschlussachen des jeweiligen Geheimhaltungsgrades ermaechtigt ist."

Bei der Abstimmung ueber die Gesetzesaenderungen gab es nur Ja-Stimmen von den Ausschussmitgliedern, die den Koalitionsparteien angehoeren, die SPD-Abgeordneten enthielten sich der Stimme, die GRUENEN stimmten nicht mit.

Arne Boernsen begruendete in seinem Brief das Verhalten der Genossen so: "Wir halten es auch fuer unverhaeltnismaessig und unpraktikabel, das bei der Durchfuehrung von Ueberwachungsmassnahmen eingesetzte Personal der privaten Diensteanbieter einer Sicherheitsueberpruefung zu unterziehen. Die Bundesregierung hat erklaert, dass nach ihrer Auffasssung schon heute jegliche Art des Fernmeldeverkehrs einer Ueberwachungsmassnahme zugaenglich sei; auch das Verfahren, private Diensteanbieter einer Sicherheitsueberpruefung zu unterzeihen, halte sie fuer praktikabel, dies sei zum Teil schon heute der Fall; die technischen Ueberwachungsmassnahmen seien durchfuehrbar, da sie in den Vermittlungsstellen der Deutschen Bundespost bzw den von privaten Diensteanbietern errichteten Netzknoten ansetzen wuerden."

Bei einem Gespraech mit Gerhard Enoch, dem Referenten der SPD in diesem Ausschuss, kam das heraus, was man schon vermuten konnte. An Mailboxen und andere moegliche Kommunikationsformen ist bei der Aenderung des Gesetzes gar nicht gedacht worden. Laut Enoch wurde von den Regierungsparteien in der Regel das Mobile Funknetz D als Beispiel angebracht.

Fallen nun Mailboxen unter unter das geaenderte Gesetz ?

Um das herauszufinden, habe ich zuerst mal ganz unbedarft bei der Pressestelle des Fernmeldeamtes Oldenburg nachgefragt. Herr von Deetzen meinte, dass ALLE Telekommunikationseinrichtungen, die an das Fernmelde-netz in welcher Form auch immer angeschlossen sind, selbstverstaendlich darunter fallen.
Also auch Mailboxen?
So explizit wollte Herr von Deetzen nicht antworten, sondern verwies mich an die juristische Abteilung der Oberpostdirektion in Bremen.

Hier wurde mir erklaert (der Name des Herrn ist mir entfallen), dass diese Frage politischer Natur sei und dass man sie in Bremen auch nicht so genau beantworten koenne. Ich moege mich doch -bitte schoen- an das Bundespost-ministerium in Bonn wenden.

In der Pressestelle des Bundesministeriums fuer Post und Telekommunikation erklaerte mir Herr Bruchmueller, dass wenn private Anbieter - auch Mailboxbetreiber - anderen (Benutzern) ihre Dienste kommerziell anbieten, fallen sie unter das G-10. Denn, so Bruchmueller, Zugang zu einer Mailbox hat ein Benutzer nur mittels eines Passwortes. Meinen Einwand, es gaebe durchaus auch Mailboxen, wo ein Gastaccount moeglich ist, lies er nicht gelten. Dies sei lediglich eine ganz seltene Ausnahme, meinte er.

Ich hielt meine Frage immer noch nicht fuer beantwortet und wandte mich an den Innenausschuss im Bundestag. Der Fachreferent der SPD, Herr Moron, konnte mir keine Auskunft geben, fand die Frage aber hoechst interessant. Im Uebrigen waere das doch alles nicht so schlimm, schliesslich wuerde das G-10 Gremium im Jahr ueber 10 bis 15 Faelle entscheiden und das seien ja nicht so viele. Alles Weitere moege ich doch -bitte schoen- mit dem Referenten des Ausschusses fuer das Post- und Fernmeldewesen, Herrn Enoch besprechen. Ansonsten koenne er mir nur noch empfehlen, mich an den Bundesinnenminister schriftlich zu wenden, er macht mich aber darauf aufmerksam, dass eine Antwort bis zu 3-4 Monaten auf sich warten lassen koennte.

Alle von mir angesprochenen Herren (!) hatten eines gemeinsam:
"Mailbox? Was ist das denn? ... Ach so, Computer! ...
"Also wissense junge Frau, da haben Sie ja doch keine Ahnung von, und dass wir noch viel weniger davon wissen, werden Sie schon nicht merken."

Uta Wilms

G10 - Nur neu aufgewaermt ?

So. Nachdem man jetzt mal die Meinung verschiedener Leute, Behoerden, Parteien, etc gelesen hat kommt jetzt nochmal meine persoenliche Meinung zu dem Thema.
Waehrend der Materialsammlung zum Thema 'G10' sind doch einige Ungereimtheiten aufgetaucht. Auch der Vorwurf, dass man jetzt ein Thema hochkocht, welches schon vor 20 Jahres ausdiskutiert wurde kam.
Warum macht man sich jetzt ploetzlich jetzt wieder Gedanken um die G10-Gesetze. Nur weil es Aenderungen gab ?

Angefangen hat alles mit der Frage, ob sich Mailboxbetreiber bei Black Penny nun anmelden muessen oder nicht. Eine Antwort koennen wir jetzt immer noch nicht geben. Bis vor 4 Tagen war ich der Meinung: Sie muessen nicht.
Diese Aussage kam vom FA Oldenburg nach Rueckfrage bei der OPD Bremen und dem BMPT. Wenn man auf diesem Wege anfragt, bleibt die Antwort auch immer gleich: Mailboxen - ob vernetzt oder nicht - brauchen nicht angemeldet werden.
Die selbe Frage an das Pressereferrat des BMPT (Bundesministerium fuer Post und Telekommunikation) gestellt, hat zur Folge das man erfaehrt, dass natuerlich auch Mailboxen sich anmelden muessen.

Was ist der Grund fuer diese Verwirrung ?
Anscheinend sind sich weder das BMPT, noch die Parteien im klaren, welche Kommunikationslandschaft sich entwickelt hat. Die Regierung hat mit dem Verweiss auf den Mobilfunk die Aenderungen eingebracht. Anscheinend ist man in der Regierung - aber auch bei der SPD - der Meinung, dass jedes Netz aehnlich organisiert sein muss, wie die Post - naemlich zentralistisch. Bestaerkt durch die Tatsache, dass dies bei Netzen wie DFN oder beim schon erwaehnten Mobilfunk dieses auch gilt machte man sich nicht die Muehe mal in die Welt zu sehen.

Das Pressereferat des BMPT behauptet:
Eine Mailbox = System wo man Nachrichten empfangen und versenden kann. Damit faellt es unter das G10.
Es gibt natuerlich auch Mailboxen, die wie eine 'Zeitung' mit Brettern organisiert sind, aber das ist selten. Solche fallen natuerlich nicht unter das G10.

Tatsache ist: Mailboxen bieten in der Regel BEIDE Dienste an. Schon haeufig wurden auf Mailboxen das Presserecht angewendet. Unter diesem Gesichtspunkt wuerde eine Ueberwachung sicher unmoeglich sein. Man stelle sich eine ueberwachte Readktion vor. Auch haben Mailboxen in der BRD schon lange keinen Seltenheitswert mehr.

Selbst wenn man diese Dinge ausser acht laesst: Wenn man tatsaechlich eine Person ueberwachen will - sollen dann ALLE Mailboxen, wo dieser Benutzer eingetragen ist ueberwacht werden ? Die Regierung geht davon aus, dass es eine zentrale Vermittlungsstelle gibt, wo alle Nachrichten weitergeleitet werden. An dieser Stelle sollte dann die Ueberwachung angesetzt werden - eben wie in der Vergangenheit bei dem Abhoeren von Leitungen in den Vermittlungszentren der alten Post.

In einem Mailboxnetz sind die einzelnen Knotenrechner in der Regel gleichberechtigt. Haben da die Politiker wiedermal an der Realitaet vorbeigedacht ?

Wie sieht es ueberhaupt mit den Universitaeten aus. Muessen diese sich anmelden ? Eine Nachfrage an der Uni Oldenburg hat nur gebracht, dass dort keinerlei Aufforderung zu einer Anmeldung eingegangen ist. Derzeit geht man davon aus, dass die zentralen Verwaltungsstellen fuer die Netze wie z.B. DFN, GMD, etc diese Anmeldung vornehmen werden. Wenn sich diese Regel bewahr-heiten sollte, dann werden wohl demnaechst auch die Vereine die fuer Zerberus und Subnet verantwortlich sind - bzw. formal nach aussen so dastehen - diese Netze anmelden muessen.

Derzeit kann man nur einen Rat geben: Weiter abwarten. Wer aber seine Mailbox umbedingt anmelden will, sollte das Gesetzt auch woertlich nehmen. Nach @26 muessen die Telekommunikationseinrichtungen bei Black Penny angemeldet werden. Also: Brief per Einschreiben und Rueckmeldung an Minister Schwarz Schilling direkt.

Es bleiben: Viele Fragen - Kopfschuetteln ueber die Realitaetferne in Bonn, und das weiterarbeiten an Codiermechanismen: Fuer alle Faelle.

Ein Kommentar noch zum Abstimmungsverhalten der SPD und der Gruenen waehrend der Beratung zu den Gesetzesaendeungen: Von einer Partei sollte man eigentlich erwarten, dass sie - im Gegensatz zu vielem Buergern - eine Meinung haben bzw. sich eine bilden. Man sollte diese Meinung aeussern: Entweder ist man fuer oder gegen ein Gesetz. Das kann man respektieren. Keine Meinung zu haben bzw. wie in diesem Fall sich der Stimme enthalten ist keine Moeglich-keit, die einer Partei gut steht.

Terra

[Contrib][Chalisti][03] G10 - Nur neu aufgewaermt ?

Verschluesseln mit Schwerpunkt DES

DES steht fuer Data Encryption Standard und stellt eine Art Daten
zu verschluesseln dar. Der DES beinhaltet den DEA Data Encryption
Algorithm. Das Ganze wurde 1976-1977 von IBM entwickelt, und 1977 als
US-Verschluesselungsstandard genormt.
Zuerst entstand in unabhaengiger Arbeit der sogenannte Lucifer-Algorithmus,
der eine Schluessellaenge von 128 Bits verwendete. Danach schaltete sich die
NSA National Security Agency ein. Sie fuehrte zusammen mit IBM die Tests
ueber die Sicherheit von DES durch, waehrend derer die Schluessellaenge
auf 56 Bit gekuerzt wurde. Berichte, was die Tests ergeben haben, sind
wie die Auswahlkriterien gewisser Interna des DEA unter Verschluss.
Es existieren aber inzwischen einige unabhaengige Studien, z.T. auf
theoretischer Ebene.

WARUM VERSCHLUESSELN ?

Zuerst mal generell: Wieso wird verschluesselt ? Naja konkret um andere
'Leute' davon abzuhalten, ihre Nase in Dinge zu stecken, die sie 'meiner'
Meinung nach nix angehen. Das koennten Rechnungen, Datenbanken, Finanz-
buchhaltungen sein. Oder Programme, die man vor der Einsicht anderer
schuetzen will, und die sich dann zur Laufzeit selbst 'decodieren'
Oder irgendwelche persoenlichen elektronische Briefe.
Natuerlich hat die Verschluessleung auch gewisse Nachteile. Wenn man
naemlich den Schluessel vergisst, ist die Information so gut wie wegge-
worfen...

Ein Rueckblick und Varianten zu DES

Die ersten detaillierten Informationen zu 'Verschluesselng' (im Gegensatz
zu den 'Geheimsprachen' von Priestern und Schamanen ist uns von den
Spartanern (400 v.Chr) ueberliefert. Da wurde von Heerfuehrern, die unter
einander geheime Nachrichten austauschen wollten ein schmaler Streifen
Pergament um einen Stab gewickelt und dann beschriftet. Der Bote kannte
diesen Trick nicht, und jemand der diese Botschaft entschluesseln wollte,
wusste also nicht, wie er die Buchstaben zu sinnvollen Worten machen sollte.
Ein Verfahren das bis anhin noch in verschiedenen Varianten verwendet wird,
schreibt man Julius Caesar zu.
Er ersetzte jeden Buchstabe des Alphabeths durch einen anderen, und legte
so regelrechte Uebersetzungs-Tafeln und -'Buecher' an. Das geht so, dass
zum Beispiel die Nachricht BRVTVS IST BOES zu CSWVWT KTV CPFT wird. Hier,
bei dieser 'Uebersetzungstabelle' entspricht ein B einem C ein I einem K
ein V einem W etc. (das koennte man zwar auch nur als eine einfache Verschie-
bung auffassen, aber schliesslich hab ich das ja im Kopf gemacht :-)
Heute werden beim Militaer bei Sprechfunkverbindungen jeweils Buchstaben resp.
Silben oder haeufige Woerter durch Zahlen oder andere Woerter ersetzt.
Schwaechen sind bei diesen (einfachen) Verfahren natuerlich vorhanden: Beim
Tauschen von Buchstaben und sogar Buchstabenpaaren nach jeweils einer
Tabelle bleiben die Haeufigkeiten von Buchstaben erhalten; das heisst mit
etwas Geschick und Kenntniss der Sprache, in der die Botschaft geschrieben
wurde, ist das Entschluesseln ohne grosse Muehe moeglich.

Es gibt fuer die Crypto-Analysis inzw. grosse 'Standard'-Werke die die

Haeufigkeiten von Buchstaben, Buchstabenpaaren, Silben und Phonemen in vielen Sprachen zur Verfuegung stellen.
In dieser Art der Verschluesselung ist man noch viel weiter gegangen. Man kann einen Text anhand mehrer Tabellen Verschluesseln. Also ueber mehrere Stufen nacheinander (z.B. ein B wird zuerst zu einem C und in einem zweiten Durchgang zu einem F), was alleine noch nicht viel bringt (zwei Ersetz-Tabellen lassen sich ja leicht auf eine zusammenfassen), aber wenn nach jedem verschluesseltem Zeichen eines Textes fuer das naechste Zeichen ein anderer Schluessel (sprich eine andere Tabelle) genommen wird, steigt die Sicherheit enorm! Je mehr verschiedene (unabhaengige) Schluessel man nacheinander verwendet, um jeweils einen Teil (Buchstaben pro Buchstaben) des Textes zu verschluesseln, desto groesser wird die Sicherheit, da nicht mal mehr Wiederholungen von Buchstabenkombinationen auftreten koennen. (Jedes Buch zur Cryptanalysis kann dazu viel mehr erzaehlen :-)
Vielleicht doch noch zwei Beispiele zu diesen Ersetztabellen:
Zuerst der heisse Draht zw. Washington und Moskau: (eine Telex-Verbindung, wie viele nicht wissen) Beim Verschicken von Meldungen von einem Ort zum andern: Jeder Buchstabe der Meldung wird nach einer anderen Tabelle verschluesselt. Es werden also jedesmal soviele Tabellen verwendet, wie der Text Zeichen hat. Das ist der einzige absolut sichere Schluessel, den man bis jetzt kennt, der nicht zu 'knacken' ist.

ENIGMA: (ein den Deutschen wohl bekannter Name fuer eine der gelungensten Chiffriermaschinen)
Die ENIGMA besteht aus mehreren Scheiben die auf beiden Seiten kreisfoermig angeordnete Kontakte enthalten. Diese Kontakte sind im Innern keuz und quer verbunden, so dass eine Scheibe eine Substitutionstabelle darstellt. Wird nun ein Buchstabe in die ENIGMA getippt, so gelangt er an die Aussenseite der ersten Scheibe. Dieses Signal kommt nun auf der anderen Seite der Scheibe an einem anderen Ort 'heraus' und gelangt auf die gleiche Art durch zwei weitere Scheiben. Dort sind die Kontakte ueber Steckverbindungen verknuepft, und das Signal wandert auf einem anderen Weg durch die gleichen drei Scheiben zurueck. Wieder auf Vorderseite angekommen, wird es dann an einem Laempchen angezeigt, und der Chiffreur erhaelt so der zu seiner gedrueckten Taste den korrespondierenden Schluesselbuchstaben. Allerdings werden nach jedem Tastendruck die Scheiben verdreht... Es handelt sich also um eine Verschluesselung mit einer maximalen Schluessellaenge von 17576 Zeichen (26^3). "Dummerweise" hatte die ENIGMA ein paar konstruktions- und gebrauchsbedingte Schwaechen, so dass den Englaendern dann eine Entschluesselung in weniger als 42000 Jahren (wie sie von den Deutschen zur Entschluesselung eines Textes veranschlagt wurden) gelang.

Heute wichtige Verschluesselungsverfahren werden normalerweise auf Computern angewendet, einfach weil die Maschinen schneller sind als Menschen. Logo.
In Diskussion stehen die Verfahren DES, FEAL und RSA. DES wird weiter unten ausfuehrlich beschrieben, FEAL ist eine stark abgespeckte Version von DES, die nichts desto trotz als aehnlich Sicher betrachtet wird. Ziel einer Verschluesselung dieser Art ist einfach, als Output einen Bitstrom zu erzeugen, der von einem zufaellig erzeugten Bitstrom nicht unterschieden werden kann. DES und FEAL scheinen das sehr gut zu erreichen.

Der Unterschied von DES zu RSA ist folgender:
- RSA bereibt zur Verschluesselung einen viel hoeheren Rechenaufwand! (Faktor 1000 ist noch untertrieben)
- RSA benutzt oeffentliche Schluessel. Das ist ein grosser Vorteil: Man kann denjenigen die einem etwas schicken wollen einfach ein paar Schluessel zur Auswahl geben, und die Verschluesseln ihren Text damit. Das hat den grossen Vorteil gegenueber DES etc. dass der Schluessel nicht geheimgehalten werden muss.

Wie RSA (Inverser Schluessel - Rivest, Shamir & Adlemann) funktioniert will ich nur ganz kurz dem Prinzip nach erklaeren. Der oeffentliche Schluessel besteht zur Hauptsache aus zwei GROSSEN (200 Stellen und mehr) Primzahlen die miteinander multipliziert werden. Will jemand einen Text entschluesseln,

muss er dazu rausfinden, wie diese zwei Primzahlen lauten. Stichwort: Faktorisierung einer Zahl. Und das das rechenaufwenig ist, wird jeder leicht einsehen.

Ein verschluesselter Text muss heutzutage nicht 'auf Ewig' geheim bleiben: Wenn jemand zum Entschluesseln nun mit den besten Rechnern zwei Wochen braucht, und man will nur einem guteen Kollgen die Lottozahlen von naechster Woche mitteilen, dann reicht die Sicherheit des verwendeten Algorithmus sicher... (na, zumindest in den meisten Faellen, bei den Lotto-zahlen wuerde wohl auch noch nach zwei Wochen ein Staatsanwalt aktiv :-)

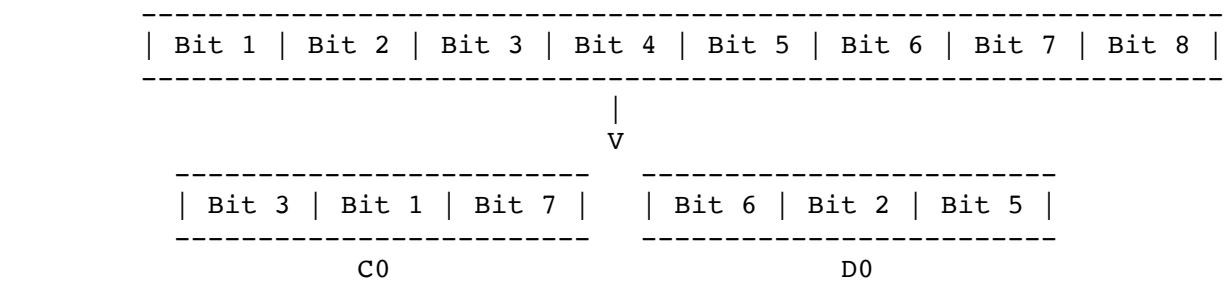
Wie funktioniert DES (DEA-Kernroutinen)

Wichtig zum Verstanedniss des DEA ist nur der eigentliche Kernalgorithmus, der jeweils 64-Bit-Blocke verschluesselt. Wie diese 64-Bit-Bloecke dann weiterhin behandelt und evt. verknuepft werden, lasse ich hier ausser acht. Es wird ein 56-Bit Schluessel und 64 Bit Daten gegeben, daraus entstehen 64 Bit Schluesseltext. Der gleiche Input erzeugt in der Kernroutine immer den gleichen Output.
DES verwendet einige Tabellen mit standardisiertem Namen. Sourcen fuer DES sind z.T als PD auf *nix-Systemen sowie VMS und VM/CMS sowie IBM's, Amigas und ST's vorhanden. (Beim Autor dieses Textes sind C-Sourcen fuer Unix,VMS,Atari,Amiga erhaeltlich)

Ablauf des DES-Algorithmus:

Der DEA teilt sich in zwei Teile. Zuerst wird nach dem folgenden Verfahren aus einem Input von 56 Bit ein DEA-interner Schluessel mit der Laenge 768 Bit generiert. Wer den DES etwas sicherer machen will, kann das ganz einfach ueber einen kleinen Trick erreichen. Er lasst dieses Expandieren des 56-Bit-Schluessel-Inputs einfach aus, und gibt direkt einen zufaelligen! 768-Bit-Schluessel vor. Das erhoeht statistisch gesehen die Sicherheit des DES um einen Faktor 2^(768-56). Aber lassen wir diese 'Details' einfach mal auf der Seite...
Aus einem 56-Bit-Schluessel (Das nierderwertigste Bit jedes Schluesselbytes geht verloren (-> 8 Bytes), respektive wird mit dem obersten Bit ver-knuepft (SUN-Implementation)) werden 16 Unterschluessel gebildet, die je eine Laenge von 48 Bit haben.
Das beginnt, indem der 64-Bit-Block des Schluessels durch die Funktion pc1 durchgeschleust wird. Dabei bleiben von den urspruenglichen 64 Bit nur 56 uebrig, die in zwei Unterschluessel C0 und D0 verteilt werden.

Kleines Beispiel :-)



Man sieht n paar Bits gehen verloren, der Rest wird wild vertauscht und zu zwei Bloecken aufgetrennt.

(56 Bit des Schluessels werden einfach nach einer Tabelle an eine andere Stelle gebracht. So wird Bit 57 des Original-Schluessels zum Bit 1 von C0, Bit 4 des Schluessels zum letzten (28-sten) Bit von D0)
Mit Hilfe dieser 2 Unterschluessel werden nun die 16 Schluessel K1 bis K16 erzeugt, indem C0 und D0 jeweils um 1 oder 2 Bit nach links rotiert werden, und dann aus diesen 56 Bit mit Hilfe der Tabelle pc2 48 Bit selektiert

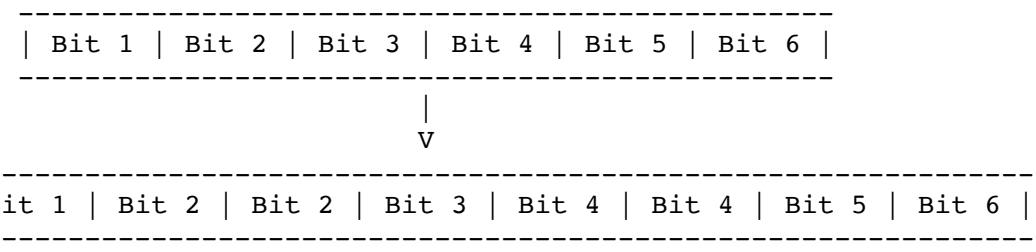
werden. Diese Bits bilden den Schluessel Ki.
Also nochmal ausfuehrlich: Wir haben Ci und Di (Am Anfang ist das C0 und D0)
Jetzt machen wir einen Shift, das heisst, wir rotieren alle Bits von Ci und
Di um ein oder zwei Stellen nach links. 1001010 -> 0010101
Jetzt setzen wir Ci und Di (nach dem ersten Rotieren koennen wir sie mit
C1 und D1 bezeichnen, wieder zusammen. Also haben wir wieder ein Bitfeld mit
56 Bit. Daraus waehlen wir anhand der Tabelle PC2 48 Bit aus vertauschen die
wild und nennen das Ergebniss Ki (Beim ersten Mal also K1) Jetzt wird wieder
rotiert, und ausgewaehlt und das ganze 16 mal. Das gibt so K1 bis K16.
Dabei wird beim ersten, zweiten, neunten und letzten Durchlauf Ci und Di um 1
Bit rotiert, sonst um zwei. Technisch gesehen:
Nach dem Rotieren kann man Ci und Di wieder als zusammenhaengend betrachten,
(Bit 1-28 Ci Bit 29-56 Di), und fuehrt darauf die Permutation pc2 aus.
Das heisst Bit 14 von CiDi wird zu Bit 1 vom Unterschluessel Ki, Bit 1 von
CiDi wird Bit 5 in Ki etc. Am Schluss bleiben so die 16 Schluessel Ki,
mit je 48 Bit Inhalt. (Anm. d. Setzers: man muss dies nicht alles im Kopf
nachvollziehen, oder..?)
Diese 16 Unterschluessels bleiben auch bei einem laengeren Verschluesselungs-
vorgang immer gleich. (Natuerlich koennte man auch dies zum steigern der
Sicherheit varieren :-)

Die Verschluesselung der 64 Bit Daten laueft nun wie folgt ab:
Zuerst wird wieder (DES macht das liebend gern) permutiert. Dieses Mal mit der
Tabelle ip. Bit 58 des Inputs wird so zu Bit 1 des Outputs etc.
Das heisst wir stecken mal unsere 64 Bit Source in die DEA-Kernroutine.
Die vertauscht diese 64 Bit wild miteinander.
Die entstehenden 64 Bit werden aufgeteilt: Bit 1-32 (DES kennt kein 0-tes
Bit) wandern nach L0, Bit 33-64 nach R0.
Also wieder ein Aufteilung in zwei Haelften, wie bei der Generierung der
Schluessel auch schon, nur dass die Haelften Li und Ri heissen ...
Jetzt kommen 16 Durchlaeufe, in denen eine Kernfunktion f(Ri,Ki) auf Li
und Ki einwirkt. Also zuerst wandern K1 und R0 in die Funktion f.
Man merke K1 war der erste Unterschluessel, den wir vorher generiert haben,
R0 ist die rechte Haelfte des soeben wild vertasuchten 64-Bit-Blocks
Diese Funktion f() macht nun 'irgendwas' mit dem Ri das reingesteckt wird.
Nach dem Durchlaufen der Funktion f() wird der Inhalt von Ri,Li vertauscht,
und R(i+1) mit Li XOR-verknuepft.
L1 ist also R0, R1 ist L0 XOR f(R0,K1). R1 ist also L0 XOR das Ergebniss
der vorher ausgefuehrten Funktion f. Kompliziert? Warten Sie mal die Funktion
f() ab...
Nun wandern R1 und K2 in die Funktion f. Das Ergebnis wird mit L1 geXORt,
und wird zu R2, waehrend R1 zu L2 wird. So geht das weiter bis alle 16
Schluessel Ki verarbeitet sind.
Die letzte Operation ist also: R15 wird zu L16 und R16 ist das Ergebnis von
L15 XOR f(R15,K16)
Am Ende werden L16 und R16 nochmal vertauscht, das heisst R16 liefert die Bits
1-32 und L16 die Bits 33-64 des Outputs, dann wandert das durch die Funktion fp
die genau das inverse der Permutation ip macht.(Also Bits wild vertasuchen:-)
Das heisst Bit 40 des Inputs wird zu Bit 1 des Outputs etc.
So entstehen 64 Bit, die das verschluesselte Aequivalent zu den 64 Input-
Bits darstellen.
Um 64 Bit zu entschluesseln, anstatt sie zu verschluesseln, laesst man genau
die gleiche Prozedur wie oben nochmal ablaufen. Mit einem Unterschied.
Die Schluessel K1 bis K16 werden nich in der aufsteigenden Reihenfolge der
Funktion f() zugefuehrt, sondern in absteigender Reihenfolge, ausserdem
werden die zwei Haelften der 64 Bit am Anfang vertauscht, bei der Bildung
von R0 und L0, und dafuer am Ende nicht.

Nun die Funktion f(Ri,Ki):
Input in diese Funktion sind 32 Bit Text und 48 Bit Schluessel.
Zuerst werden die 32 Bit Text zu 48 Bit aufgeblasen. Das geschieht mit
der Funktion ei, die bei mir (nach einer Idee die ich Ende September
in einer Anleitung zum SUN-DES gefunden habe, und die den gesamten
Verschluesselungsvorgang um etwa den Faktor 8-10 schneller macht) implizt

in der SP-Permutation enthalten ist. Auch die Permutationen S und P,
siehe weiter unten, sind bei mir zu einem 2D-Array zusammengesetzt, in dem
alle Moeglichkeiten tabellarisch behandelt werden.
Zur Erklaerung beschreibe ich jetzt trotzdem, wie die Definition des
Algorithmus die Funktion f() durchfuehrt, die Beschreibung meiner Methode
ist im Listing eingebunden und mit dem dazugehoerigen Programmtext auch
viiiiel verstaendlicher.
Also. Wir fangen an mit 32 Bit Text und 48 Bit Schluessel.
Diese 32 Bit Text muessen auf 48 Bit expandiert werden. Das geschieht
indem verschiedene Bits doppelt gezaehlt werden; das besorgt die Funktion
ei. Wir haben nach Benutzen von ei 48 Bit Text und 48 Bit Schluessel.

Das Expandieren sieht vereinfacht so aus:



Nun haben wir also einen Schluessel und einen aufgeblasenen Input:
Darauf wird ein XOR ausgefuehrt. Nun werden die entstehenden 48 Bit
in 8 6-Bit-Haeppchen aufgeteilt. Jedes dieser 6-Bit-Haeppchen wird in einer
der 8 S-Boxen zu 4 Bit Output reduziert. (Die S-BOX S1 ist fuer die ersten 6
Bit zustaendig, die S-Box S8 fuer die letzten 6 Bit) Man stelle sich unter
einer S-Box eine Tabelle mit vier Reihen und 16 Spalten vor. Jeder Tabellen-
eintrag besteht aus einer Vier-Bit Zahl. Um einen Tabelleneintrag anzusprechen,
braucht man 6 Bit (2 Bit geben die Reihe 1-4 an, 4 Bit die Spalte 1-16) Wenn
man nun am so bestimmten Ort der S-Box hineingreift, erhaelt man eine 4-Bit-
zahl, die man als Output der S-Box bezeichnet.
Dabei geben (bei der Tabellen-Version) das erste(lo) und das letzte(hi)
Bit die Reihe der S-Box an (z.b. 0xxxx0 1.Reihe 0xxxx1 2.Reihe etc)
und die mitteleren vier Bits die Spalte (0-15) der S-Box.
Der Wert 110100 (3. Reihe, 10. Kolonne) in der ersten S-Box wuerde also
in den Wert 1001 (9) umgewandelt werden. Aus 6 Bit Input entstehen dabei
4 Bit Output! Nun werden diese entstandenen 8 Nibbles (a 4 Bit) durch die
Permutation P32i auf die 32 Bit endgueltigen Output der Funktion f
verteilt (Bit 1 des ersten Nibbles geht zu Bit 16 des Outputs etc), also
nochmal alles wild miteinander vertauscht, und das leifert f(Ri,Ki) dann
dem Aufrufenden als Output zurueck. Un das war auch schon alles. So zum Lesen,
ist das Ganze natuerlich irre kompliziert, aber im Programm sieht man recht
bald, was so vor sich geht...

AUFWAND DES DEA

Wie man anhand des Technischen Beschriebs von vorher wohl merkt, ist die
Realisierung mit rein softwaremaessigen Mitteln verhaeltnissmaessig
rechenaufwendig. Es lassen sich aber, duch Aufbau von ein paar trickreichen
Tabellen, viele dieser Bitvertauschungen in einfache indizierte Abbildungen
und Verkuepfungen (OR's) umwandeln.

- Literaturverweise

Data Encryption Standard Federal Information Processing Standards (FIPS)
Publication 46, US Department of Commerce / National Bureau of Standards,
Jan. 15,1977

Validating the Correctness of Hardware Implementations of the NBS Encryption
Standard NBS Special Pubilcation 500-20, US Department of Commerce/ National

Bureau of Standards, 1977

Katzan, H. The Standard Data Encryption Algortihm, Petrocelli Books Inc,
New York, 1977

BYTE Publications March 1979 The DES, An Overwiew, Robert V Meushaw

Horster P. Kryptologie, Bibliografisches Institut, Reihe Informatik Bd. 47

Structure in the S-Boxes of the DES (extended abstract) E.F. Brickwell/
J.H. Moore/M.R. Purtill

... weiteres theoretisches Material beim Vortragenden erhaeltlich
    Meine Ur-Quelle: CCC (Dank an Bernd Fix + Frank Simon)

Autor Germano Caronni fuer die Chalisti 3 (Dezember 1989)

[Contrib][Chalisti][03] Verschluesseln mit Schwerpunkt DES

IBM VM/SP: CMS Release 5 - Eine Einfuehrung

INHALT
======

TERMINAL
========

Anders als beim PC oder den meisten anderen Grossrechner arbeit die IBM mit intelligenten Terminals, das bedeutet:
Man ist z.B. im Editor und gibt einen Text von mehreren Zeilen ein, aendert hier mal was und dort korrigiert man einen Tippfehler. Das alles wird vom Terminal erledigt, und erst wenn man die Freigabe-Taste drueckt wird der gesamte (geaenderte) Bildschirminhalt zur Verarbeitung an den Grossrechner geschickt. Dies entlastet den Rechner natuerlich von so profanen Sachen wie Cursorsteuerung o.ae.

Nach der ueblichen Einlogprozedur mit Benutzerkennung und Passwort befindet man sich bei einem unfreundlichen System nur im CP und muss noch CMS laden, ein freundliches System nimmt einem dieses ab.

GERAETE
=======

Geraete sind Konsole, Drucker, Reader, Minidisks (MD) u.ae.
Identifiziert und angesprochen werden sie ueber Nummern. Die Konsole hat z.B. (meistens) 009, Drucker 00E, Reader 00C und die MD 191.
Auf Minidisks anderer Benutzer wird mit dem LINK-Befehl zugegriffen (damit sind sie erstmal irgendwie da und durch eine Nummer identifiziert) und die Files darauf mit dem ACCESS-Befehl (damit hat die MD und die Files darauf einen Filemodus).
Minidisks sind durch Lese- und Schreib-Passwoerter geschuetzt.

FILES
=====

Identifiziert werden Files durch Namen, Typ und Modus. Name und Typ duerfen bis zu 8 Zeichen lang sein, kaum Sonderzeichen (z.B. ".", " " nicht) enthalten, der Filemodus besteht aus einem Buchstaben und einer Zahl. Die Zahl gibt die Leseberechtigung an: 0 sind private Files die nur

bei Schreibrecht gelesen werden koennen, 1 und 2 sind oeffentlich, 3 ist "Read once": Bei Schreibrecht wird das File nach einmal Lesen geloescht.
Wildcards beim Lesen sind:
% als Joker fuer ein beliebiges Zeichen, * fuer beliebige Zeichen.
Bei der Ausgabe (Copy, Rename, ...)uebernimmt = den alten Wert
Filetypen klassifizieren die Files, z.B.

EXEC	In den Kommandosprachen EXEC 2 oder REXX geschriebenes Programm und als (CMS-) Befehl aufrufbar.
MODULE	Programm in Maschinensprache oder Compilate
XEDIT	wie Typ EXEC, aber als XEDIT-Befehl nur im XEDIT aufrufbar.

BEFEHLE (allgemein)

Gross/Kleinschreibung ist im Prinzip egal da alle Eingaben in Grossbuchstaben umgewandelt werden. Mit einem Trick koennen jedoch von einem Programm aus Kleinbuchstaben verwendet werden...

Es gibt drei Arten von Befehlen:
1) Files
   a) EXECs (Kann auch ausgeschaltet werden, dann werden sie mit dem CMS Befehl EXEC gestartet)
   b) MODULEs
2) CMS-Befehle
3) CP-Befehle

die auch in dieser Reihenfolge abgeprueft werden (allerdings gibt es noch einige Zwischenstufen, aber dies ist die grobe Struktur).
Eingebaute Befehle koennen hiermit durch selbsgeschriebene Programme ueberlagert werden, wobei der urspruengliche Befehl immer noch benutzt werden kann.

Eingebaute Befehle koennen abgekuerzt werden und sind der englischen Sprache entlehnt. Fuer jeden Befehl (also auch Files) kann man Synonyme anlegen und sagen, wieweit sie abgekuerzt werden duerfen.
Aufgerufen werden sie mit
BEFEHL Argument1 Argument2 ... (Option1 Option2 ...)

SPEZIELLE BEFEHLE

COPY fn ft fm nfn nft nfm (optionen
Kopiert ein File. Moegliche Option z.B. REPLACE zum Ueberschreiben des Zielfiles oder APPEND zum Anhaengen an ein vorhandenes File.
CP
Umgeht CMS und gibt den Befehl sofort an das CP weiter
ERASE fn ft fm
Loescht ein File; ERASE * * fm wird abgefangen|
EXEC
Fuehrt ein EXEC-File aus
FILELIST name typ modus
Zeigt alle Files an, auf die Name, Typ und Modus zutreffen.
FILEL CHALISTI AUSGABE% *
zeigt z.B. alle Files mit Filenamen CHALISTI und einem Filetyp der mit AUSGABE anfaengt und noch ein Zeichen hat, z.B. AUSGABE2 .
In der Filelist kann einfach mit den Files gearbeitet werden:
Man geht in die Zeile, in der das Files steht, schreibt seinen Befehl in die Zeile und anstatt des Filenames setzt man einfach ein / bei dem Befehl, z.B. schreibt man in die Zeile mit CHALISTI AUSGABE2 A1
COPY / = AUSGABEN B (APP
wird das File CHALISTI AUSGABE2 A1 an das File CHALISTI AUSGABEN B angehaengt.
HELP

Auf diesen Hilfeschrei hin wird einem ein schoenes Menue praesentiert aus dem man sich aussuchen darf, ueber welches Gebiet man Hilfe moechte. Und so geht es von Menue zu Menue. Wenn man natuerlich schon genau weiss, wozu man Hilfe braucht, kann man das auch gleich angeben. Entweder Hilfe zu einem bestimmten Befehl oder zu einem bestimmten Bereich ("TASK"), z.B. Editieren von oder Umgang mit Files. Es gibt aber auch HELP HELP. Da wird einem dann der Help-Befehl erklaert.

NOTE nickname/user at node
Laesst einen eine Nachricht an einen anderen Benutzer schreiben und abschicken.

PEEK
Anschauen eines Readerfiles

PRINT fn ft fm
Druckt ein File aus

QUERY
Damit kann man viele tausend Sachen ueber sein (CMS QUERY) oder das (CP QUERY) System abfragen. In CMS erhaelt man z.B. mit Q DISK oder Q SEARCH Informationen ueber angesprochene Platten, im CP z.B. mit Q NAMES eine Liste der aktiven Benutzer, mit Q USER userid den Status eines bestimmten Benutzers (Logged on, not logged on oder disconnected), mit Q TIME die Zeit und mit Q VIRTUAL Info ueber angeschlossene virtuelle Geraete.

RDRLIST
Zeigt einem die Files im Reader an, aehnlich wie FILELIST.

RECEIVE
Empfangen eines Readerfiles auf eine Minidisk

RENAME fn ft fm nfn nft nfm
Umbenennen eines Files; ein anderer Filesmodusbuchstabe (entspricht kopieren) ist nicht moeglich

SENDFILE fn ft fm TO nick/user at node
Verschickt ein File an andere Benutzer

SET
Einstellen einiger Systemsachen, z.B. SET MSG OFF um das Empfangen von Nachrichten abzuschalten.

TELL user at node Nachricht
Sendet einem anderen Benutzer eine Nachricht

XEDIT fn ft fm
Aufruf des Bildschirmorientierten Editors.

Glossar

- CMS
  (Conversational Monitor System)
  Laeuft unter CP und arbeitet mit der virtuellen Maschine
- CP
  (Control Program)
  Laeuft unter VM und arbeitet mit der realen Maschine (Rechner)
- Disconnected
  Nicht online am Terminal arbeitend sondern ein Programm laeuft selbstaendig ohne Terminalverbindung.
- EXEC 2
  "Kommandosprache" von IBM (Interpreter) zum Betriebssystem nahen Programmieren. Erweiterung von EXEC.
- IBM
  (Immer Besser Manuell)
  Firma, die die Kisten und Software liefert
- Logged on
  Benutzer ist ueber Terminal online mit dem Rechner verbunden
- Minidisk
  Virtuelle Platte; Einem Benutzer ist ein Bereich einer grossen Festplatte zugewiesen
- Reader (virtuell)
  virtueller "Kartenleser" der gesendete Files und Post enthaelt

- REXX
  (Restructured eXtended eXecuter language)
  Nachfolger von EXEC 2, nichtkompatibel.
- User
  Benutzer; Mensch, der am Rechner sitzt und arbeitet
- Userid
  Benutzerkennung/identifikation
- VM
  (Virtual Machine)
  Jedem Benutzer wird vorgegaukelt, er haette einen eigenen Rechner
  ganz fuer sich alleine, d.h. er bekommt eine "Virtuelle Maschine"
- VM/370
  Basis, auf die VM/SP aufbaut. 370 ist die Maschinensprache.
- VM/SP
  (VM/System Product)
  Programmpaket, das CP, CMS u.a. enthaelt; Erweiterung zu VM/370
- XEDIT
  Schirmorientierter Editor

LITERATUR

Wer mehr wissen will, dem sei die "VM/SP LIBRARY ans Herz gelegt,
vor allem: CMS PRIMER und die diversen GUIDEs und REFERENCEs.
Erhaeltlich von IBM oder beim freundlichen RZ-Personal.

Die 17.5 te KIF in Oldenburg

oder : Am Anfang war der Heinz, und Heinz sagte, es werde KIF
und alles ging schief.

Wie der Untertitel schon sagt, hatten wir - die Oldenburger - einige Probleme bei der Organisation. Keine Leute, keine Schlafplaetze und keine Motivation (oder doch ?).
Puenktlich am Mittwochmorgen hatten wir dann einige Schlafplaetze bei freundlichen Mitmenschen und einige offene Fragen :
Ist Oldenburg touristisch interessant, sprich, kommen die erwarteten 180 Leute, und wenn ja wohin mit ihnen ?
Nun denn, es kamen knapp 80 (nur !!!) und der Schlafplatzad-ministrator (Joerg C.) staunte nur.

Anfangsplenum 18:00.

Beginn war allerdings (wie ueblich) 19:00, anwesend etwas ueber 60 Personen.
Anschlieszend Fete (5 x 30 Haake Beck in der 330 ccm Klasse).

Naechster Tag 10:00 Arbeitskreise:

Fruehstueck 24 Stunden taeglich, Lukasz und Anhang nicht anwesend => kein Ost-West AK (Zitat " Es war dunkel draussen, also haben wir weitergeschlafen " : Die Rolladen waren runter).

20:00 Podiumsdiskussion Computer und Psyche :
War wohl nix ? Dafuer Workshop ueber Technologietransfer und Kino-film.

Freitag : Wie gehabt, 24 Stunden Fruehstueck und Arbeitskreise

20:00 Podiumsdiskussion Computer und Schule :

Findet sie statt oder nicht, war eine der Fragen zu dieser Ver-anstaltung. Aber trotz Schwierigkeiten im Angebot. (Spaeter ist dazu Bericht)

Samtag : Erst Fruehstueck dann Dangast (Anm. d. Red.: Ort an Nordsee) und Rhabarberkuchen, spaeter Abschluszplenumum 18:00 (siehe oben).
Nach der Arbeitskreisergebnissbekanntgabe (tolles Wort) kam es zum TOP Resolutionen. Ploetzlich war niemand mehr da !! (Denk !)
Nach und nach trudelten satte Studierende ein und man konnte an Fete denken.

Sonntag : Erst Fruehstueck , dann Abreise. q.e.d.

Dann 16 Stunden Schlaf und wieder hinein in die Fachschafts-arbeit. Woher kommt blosz dieser Drang, etwas tun zu muessen?

Zur Podiumsdiskussion hier mal das Thesenpapier, vom Menschen "der die KIF nach Oldenburg holte":

Die modernen Informationstechnologien ziehen in immer staerkeren Masze

auch in die Schulen ein. Der allgemeine Kniefall vor den neuen Technologien macht auch vor ihren Tueren nicht halt. Die Kultusministerien machen Gelder locker, um den Computer in die Schulen zu bringen. Die Unternehmen der Computerindustrie sehen dies mit Freuden und setzen viel daran, ihre Produkte dort abzusetzen. Dabei wird oft und gerne "vergessen", ueber den paedagogischen Sinn bzw. Unsinn dieser Entwicklung nachzudenken.
Dieses geht nicht, ohne sich ueber die Ziele der Schule klar zu werden: Was sollen unsere Schulen eigentlich? Ist eine Schule ...

- eine berufsqualifizierende Einrichtung, die es den Absolventen moeglich einfach machen soll, sich in den Arbeitsprozesz einzugliedern?
- Die Chance fuer jedeN einzelneN SchuelerIn, sich selbst zu verwirklichen und individuelle Faehigkeiten zu entwickeln?
- oder vielleicht auch die Basis fuer die Fortentwicklung des menschlichen Zusammenlebens auf der Grundlage der Erziehung des einzelnen zu verantwortungsbewusztem Handeln und Denken?

Diese Frage ist sicherlich entscheidend bei der Diskussion ueber Computer im Schulzimmer.

Auf der anderen Seite ist die Frage nach Computern in der Schule auch nach den Anwendungen zu beurteilen. So sollte man grob drei Anwendungsrichtungen unterscheiden:

1) der Computer als Lehrwerkzeug (z.B. sog. tutorielle Systeme)
2) der Computer als ("interaktives") Medium
3) die Informatik als Unterrichtsgegenstand

Betrachtet man diese drei Gebiete naeher, so sind folgende Schlusz-folgerungen naheliegend:

1) Der Computer als Lehrwerkzeug (CUU, Computer unterstuetzter Unterricht) ist abzulehnen. Die SchuelerInnen werden in ihrem Lernen beschraenkt auf die Systematik des Computers. Der fuer die soziale Entwicklung wichtige Kontakt zum/zur LehrerIn wird stark eingeschraenkt.

2) Der Computer als Medium sollte nur sehr sparsam eingesetzt werden. Der Versuch, komplexe Vorgaenge z.B. durch Computersimulation durch-schaubar zu machen, foerdert die Akzeptanz von Scheinwirklichkeiten, neuen Realitaeten; die durch die anscheinend leichte Beherrschbarkeit oft zur Flucht aus dem Alltag genutzt werden (vgl. z.B. die Veroeffent-lichungen von W. VOLPERT). Die Moeglichkeiten, die der Computer fuer das individuelle Arbeiten bietet (z.B. Textverarbeitung, Tabellenkalkulation) sind in allgemeinbildenden Schulen nicht notwendig.

3) Die Wichtigkeit der Informatik als Lehrinhalt wird oft ueberschaetzt. Die heute ueblichen Programmierkurse sind abzulehnen, da sie nur kurz-lebige Berufsqualifikationen schaffen, die nur wenige brauchen (denen diese Kentnisse ohnehin in kurzer Zeit beigebracht werden koennen). Ohne Zweifel ist, dasz die Schule sich mit der Computertechnik auseinandersetzen musz. Wichtiger jedoch als blosze Vermittlung technischer Kentnisse erscheint jedoch die begleitende Betrachtung soziologischer, psychologischer und oekonomischer Erscheinungen.

Dies schlieszt die Betrachtung von Gebieten der sog. Kerninformatik nicht aus, im Gegenteil, durch die Vermittlung informatikbezogener Grund-kentnisse koennen SchuelerInnen lernen, sich mit der Technologie fundiert auseinanderzusetzen (z.B. ist es wichtig zu zeigen, dasz Computer keineswegs "denkende Wundermaschinen" mit dem Anspruch der Unfehlbarkeit sind).

Diese Aspekte werden in der technokratisch gepraegten Diskussion zu Computern in der Schule zu wenig beachtet. Ich moechte zum Schlusz noch einmal daran erinnern, dasz die Paedagogik, die Erziehung zum kritisch

handelnden und in die Umwelt gestaltend eingreifenden Menschen im Vordergrund stehen musz, und sich die Frage nach Computern im Unterricht nur so stellen darf: Wie kann der Computer meine paedagogische Arbeit unterstuetzen?; und nicht: Der Computer kann dieses und jenes, wie kann ich meine Paedagogik darauf ausrichten, dieses zu benutzen?!

Paperware und Ankuendigung

Das Protokoll der KIF, sowie die folgenen Anlagen sind vorhanden:

- OST-WEST (bzw. BRD-DDR) (Anlage A)
- Neue Rechte (Anlage B)
- Erstsemestereinfuehrung (Anlage C)
- Feyerabend (Anlage D)
- AK GI-Jahrestagung (Anlage E)
- Marks D. Sibanda (Anlage F)
- AK "GO go home" (Anlage H)
- Resolution zum Tod von Conny Wessmann
- Resolution zur Anerkennung der DDR-Staatsbuergerschaft
- Workshop-Protokoll "Osten, Westen, Dritte Welt:Technologietransfer"
- Protokoll der Podiumsdiskussion "Computer und Schule"

Wer die haben moechte (z.B. fuer andere Informatikfachschaften) wende sich an:
100412@DOLUNI.bitnet (x)or ...!unido!uniol!fsinfo.UUCP.

Wo, Wann, Was, Wie die naechste KIF ?

Die Kieler Fachschaft (bzw. Kay) haben vorgeschlagen, die naechste KIF ausrichten. Da es keine Alternativ-Vorschlaege gibt, wird dieser Vorschlag einstimmig angenommen.
Als Termin wird die Zeit vom 9. bis 13. Mai 1990 festgelegt.

Folgende AK's wurden fuer die 18. KIF angekuendigt:
Verhaeltnis KIF-GI
Erstsemesterarbeit
Netzwerke (EARN/UUCP)
Datenbank zwecks studentischer Kooperation zwischen Ost und West
Neue Rechte
Selbsterfahrung
Zukunftsangst
Zen oder Die Kunst, Informatik zu treiben
Computersucht
Terrorismus, "Deutscher Herbst"
Angepaszte Technologie

Joerg Cassens, Achim Kruse und andere Fachschafter ...

!Kurzmeldungen!

1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1

Ziele und Verantwortung der Informatik

Die Diskussion zum Thema Verantwortung der Informatiker, Aufgabe der Informatik, etc ist wieder neu entfacht.
Im Band 12, Heft 12, Okt 89 der Ausgabe des Informatik-Spektrums aeussern sich gleich mehrere Personen dazu.

Prof. Lenk von der Uni Karlsruhe schreibt unter dem Titel 'Koennen Informationssysteme moralisch verantwortlich sein' einen Beitrag ueber die Gefahr durch Informationssysteme im allgemeinen. Betrachtet dies aber hauptsaechlich vom philosphischen Standpunkt.

Prof. Coy von der Uni Bremen schreibt einen Artikel ueber die 'Theorie der Informatik'. Allerdings spricht er nicht ueber die theoretische Informatik wie man un meinen koennte. Seiner Meinung nach ist die Informatik keine Ingenieur- oder Naturwissenschaft, sondern eigentlich eine neue Form der Wissenschaft. Nur die Informatik hat in fast allen Bereichen eine DIREKTE Auswirkung auf die Gesellschaft, das soziale Umfeld, die Arbeitswissenschaft und politische Wirkung. Coy's Auffassung geht sogar so weit, dass er meint, dass diese Fehl-Einschaetzung der Informatik ueber sich selber die Hauptursache der Softwarekrise Anfang der 70iger Jahren war und nicht - wie bishin immer angenommen - die unstrukturierte und undokumentierte Programmierung. Sollte er damit Recht behalten, dann ist durch die Einfuehrung des Software-Engineerings und Sprachen wie Pascal die Softwarekrise nur erstmal witer aufgeschoben und nicht geloesst.

Eine vollkomme andere Meinung vertritt Dr. Luft von der Uni Erlangen. Er sieht die Informatik nur als Technikwissenschaft.

Als letztens schreibt Dr. Witt von der Firma PCS ueber die Angemessenheit der Technik-Kritik im Bereich der Informatik. Er versucht einen Bezug zwischen Technik-Kritik z.B. bei der Einfuehrung der Eisenbahn und der heutigen Kritik zu fassen und damit die Kritiz weitgehend zu entkraeften.

Auf jeden Fall fuer Interessierte aus dem Bereich Informatik, die sich auch paar warem Gedanken um ihren Beruf machen sind diese Artikel sicher eine Bereicherung.

2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2

Bonn will Computer schuetzen .

Bonn(AP). Computersysteme in der oeffentlichen Verwaltung, aber auch in der Bundesrepublik sollen kuenftig besser gegen Spione, Hacker und andere Computer-kriminelle geschaetzt werden.Das Bundeskabinett verabschiedete am Donnerstag den 23.11.89 in Bonn ein Rahmenkonzept fuer die Computersicherheit.Es sieht unter anderem den Aufbau einer Zentralstelle fuer Sicherheit in der Informat-tionstechnik (ZSI) beim Bundesministerium und die Einstufung von Computer-systemen nach Sicherheitskriterien vor.

Wie der Staatssekretaer im Innenministerium, Hans Neusel, vor Journalisten

erlaeuterte, zieht die Bundesregierung mit der Vorlage des Konzepts auch die Konsequenz aus dem Spionagefall von 1988, bei dem Hacker von Hannover aus in Computernetze in der ganzen Welt eindrangen und das erworbene Wissen- so die im August erhobene Anklage-dem sowetischen Geheimdienst KGB verkauften.

In der oeffentlichen Verwaltung der Bundesrepublik sind nach Schaetzungen des Innenministeriums derzeit etwa 50000 Computer im Einsatz.Der Wert der in der Bundesrepublik betriebenen mittleren und grossen Computer wird auf 50 Millarden DM geschaetzt; der Wert der darauf laufenden Programme auf das Doppelte.Manipulationen an diesen Systemen, Sabotage oder Spionage koennen unuebersehbare Schaeden verursachen.Die neue Zentralstelle, deren Gruendung noch in dieser Legislaturperiode durch Gesetz geregelt werden soll, soll in Zusammenarbeit mit der Wirtschaft und in Kontakt mit EG und NATO geeignete Sicherheitsstandards entwickeln.

SICHERHEITSZERTIFIKATE GEPLANT
Fuer Geraete und Programme sollen Sicherheitszertifikate vergeben werden. Je nach Anwendungsbereich werden dann nur solche Computer zugelassen sein, die bestimmte Mindesanforderungen erfuellen.

3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3

Chaos Communication Congress 1989
Das Treffen fuer Datenreisende, Hacker und Netzwerker!
Vortraege, Workshops, Hackcenter, Archiv, Chaos Cafe, Video- & Papercopiers.

Was Wann Wo: 6. Chaos Communication Congress, vom 27. bis 29.Dezember 1989
im Eidelstedter Buergerhaus, Elbgaustr. 12, D-2000 Hamburg 54

Themen(u.a.): Mailboxnetze,andere Netze und oeffentliche Datenbanken
Telefonnetz der DDR und Planung von Datenreisemoeglichkeiten
Freedom of Information Act und Copyright
Feminines Computerhandling
Cyberpunk, Viren, Wuermer, Wanzen, Datenschutz
Postreform
Zu den Diskussionen wurden kompetente in- und auslaendische Gaeste eingeladen.

Teilnahme:

CCC Mitglieder	23,- DM
Private Teilnehmer	33,- DM
Kommerzielle Teilnehmer	103,- DM
Presse	53,- DM

Die Teilnahmegebuehr gilt fuer alle Congresstage und Veranstaltungen. Nur Pressevertreter benoetigen ein Passfoto! TV-Teams moegen sich bitte anmelden.
DDR-Buerger mit gueltigem Visum koennen Eintritt, Mitgliedschaft, Datenschleuder-Abos und Kaffee mit Ostmark (1:1) bezahlen!

Voranmeldung: Durch Ueberweisung auf das Konto 59 90 90 - 201 des Chaos Computer Clubs beim Postgiroamt Hamburg (BLZ 200 100 20). Einzahlungsbeleg dient als Quittung fuer die Teilnahme (also bitte mitbringen).

Vor Ort: Ab dem 27. Dezember, 14 Uhr sind wir auf dem Congress erreichbar.

Projektleitung/Zentrale	040/570 8228
Pressestelle	040/570 3664
Telefax	040/570 6765

Kontakte/Infos:

CCC ServiceCenter (Di+Do Nachmittags)	040 /4903757 Q
Pressearbeit (J.Wieckmann)	040 /275186
Organisation (S.Wernery)	040 /483752 Q

Telekopie 040 /4803181
Chaos-Berlin (West) (Helmut) 7531579

Wir suchen noch Kontakte zu Computerfans und -clubs in der DDR. Bitte meldet euch!

4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4

Chalisti - wie geht's weiter

So. Die 3te Chalisti ist fertig. Wir moechten uns bei denen bedanken, die uns Artikel und Material geschickt haben. Es ist das erstemal, dass nicht alles in die Chalisti kam. Die Texte sind aber nicht verloren gegangen. Mindestens in die Chalisti 5 werden die Texte dann aufgenommen werden. Die Chalisti 4 wird die Congress-Chalisti sein. Zusammen mit der Redaktion Datenschleuder, einigen freiwillig Zwangsverpflichteten und uns werden wir auf dem Congress im Erdgeschoss in der Redaktion hocken und versuchen moeglichst viele Artikel ueber die Geschehnisse auf dem Congress zu schreiben bzw. aufzutreiben. Diesesmal wollen die Redakteure aber auch etwas vom Congress haben, deswegen waere es nett wenn Congress-teilnehmer mal kurz in der Redaktion hereinschauen koennten und sich dazu melden ueber ein oder zwei Workshop's zu schreiben.

Dann wollte ich nochmal darauf aufmerksam machen, dass die Adresse Chaos Computer Club, Uni Oldenburg zwar ganz nett klingt, aber nur mit sehr viel Glueck ankommt. In diesem Fall ist irgendein Brief verschwunden. Beschraenkt euch doch bitte auf die im Impressum angegebenen Kontakt-moeglichkeiten.

Redaktion Chalisti

IMPRESSUM

"Die gesamte Menschheit bleibt aufgefordert, in freier Selbstbestimmung
die Einheit und Freiheit des globalen Dorfes zu vollenden."

Herausgeber: Chaos Computer Club e.V./Redaktion Chalisti

V.i.S.d.P. : F.Simon

Redaktion: Volker Eggeling, Frank Simon

Mitwirkende an dieser Ausgabe:
Uta Wilms, Michael Niermann, Andy, Ikarus, Peter Lobenstein,
Germano Caronni, Jochen Ries, Achim Kruse, Joerg Cassens,
u.a.

Redaktionen: Chalisti, c/o Frank Simon, Kennedystr. 12, 2900 Oldenburg
Tel. 0441/592607
Datenschleuder, Lachswehrallee 31, 2400 Luebeck
MIK-Magazin, c/o J. Wieckmann, Barmbeker Str.22, 2000 HH 60
Tel. 040/275186

Verbreitung: Zerberus : /Z-NETZ/CHALISTI
UUCP(dnet) : dnet.general
UUCP(sub) : sub.org.ccc
EARN/Bitnet: CHAMAS@DOLUNI1, Brett CHALISTI
GeoNet : mbk1: brett ccc-presse
FidoNet : ccc.ger
MagicNet : Artikel&News

Adressen: EARN/Bitnet: CHAMNT@DOLUNI1
UUCP : eggeling@uniol (eunet)
chalisti@olis (subnet)
Zerberus : terra@mafia
GeoNet : mbk1: chaos-team
FidoNet : Volker Wieners on 2:241/2.1205

Teilnehmer aus diversen anderen Netzen wie z.B. ArpaNet,
DFN, etc. nutzen bitte die Bitnet Adresse ueber das
entsprechende Gateway.