die datenschleuder.

Das wissenschaftliche Fachblatt für Datenreisende / Ein Organ des Chaos Computer Club

- Staatssicherheit aufgelöst oder das Operationsgebiet eingenommen?
- SecurEdoc bei TNT: Ein kleiner, feiner Hack und ein mittlerer Datenschutzskandal
- Dummheit - ein grausamer, globaler Gott
- Machtstrukturen und Zensur im Internet

ISSN 0930.1045 • Frühjahrsimulation 2001
dm 5,- (see the pattern?)
Postvertriebsstück C11301F

074

Erfa-Kreise

Hamburg

Lokstedter Weg 72, D-20251 Hamburg, *mailto:mail@hamburg.ccc.de./ http://hamburg.ccc.de* Phone: +49 (40) 401 801-0 Fax: +49 (40)401 801 - 41 Voicemailbox +49 (40) 401801-31. Treffen jeden Dienstag ab ca. 20.00 Uhr in den Clubräumen. Der jeweils erste Dienstag im Monat ist Chaos-Orga-Plenum (intern), an allen anderen Dienstagen ist jede(r) Interessierte herzlich willkommen. Öffentliche Workshops im Chaos Bildungswerk fast jeden Donnerstag. Termine aktuell unter *http://hamburg.ccc.de/bildungswerk/.*

Köln

Chaos Computer Club Cologne (c4) e.V.
Vogelsangerstraße 286 / 50825 Köln
50°56'45"N, 6°51'02"O (WGS84)
http://koeln.ccc.de/ Tel. 0221-5463953
mailto:oeffentliche-anfragen@koeln.ccc.de
Treffen Dienstags 20:20

Berlin

Club Discordia jeden Donnerstag zwischen 17 und 23 Uhr in den Clubräumen in der Marienstr. 11, Hinterhof in Berlin-Mitte. Nähe U-/S-Friedrichstraße. Tel. (030) 285986-00, Fax. (030) 285986-56. Briefpost CCC Berlin, Postfach 640236, D-10048 Berlin. Aktuelle Termine unter *http://www.ccc.de/berlin*

Ulm

Kontaktperson: Frank Kargl <frank.kargl@ulm.ccc.de>
mailto:mail@ccc.ulm.de / http://www.ulm.ccc.de/
Treffen: Montags ab 19.30h im 'Café Einstein' in der Universität Ulm.
Vortrag chaos-seminar: Jeden ersten Montag im Monat im Hörsaal 20 an der Universität Ulm.

Bielefeld

Kontakt Sven Klose Phone: +49 (521) 1365797, *mailto:mail@bielefeld.ccc.de.*Treffen Donnerstags, ab 19.30 Uhr in der Gaststätte 'Pinte', Rohrteichstr. 28, beim Landgericht in Bielefeld. Interessierte sind herzlich eingeladen.

Chaos-Treffs:

Aus Platzgründen können wir die Details aller Chaos-Treffs hier nicht abdrucken. Es gibt in den folgenden Städten Chaos-Treffs, mit Detailinformationen unter *http://www.ccc.de/ChaosTreffs.html*.
Bochum/Essen, Bremen, Burghausen /Obb. und Umgebung, Calw, Dithmarschen/Itzehoe, Dresden, Emden / Ostfriesland, Eisenach, Erlangen /Nürnberg/Fürth, Frankfurt a.M., Freiburg, Freudenstadt, Giessen/Marburg, Hanau, Hannover, Ingolstadt, Karlsruhe, Kassel, Lüneburg, Mannheim /Ludwigshafen/Heidelberg, Mönchengladbach, München, Münster/Rheine/ Coesfeld /Greeven/Osnabrück, Rosenheim /Bad Endorf, Neunkirchen/ Saarland, Würzburg, Schweiz /Dreyeckland: Basel, Österreich: Wien

Impressum

Herausgeber

(Abos, Adressen, etc.)
Chaos Computer Club e.V.
Lokstedter Weg 72, D-20251 Hamburg
Tel. +49 (40) 401801-0, Fax +49 (40) 401801-41,
mailto:office@ccc.de

Redaktion

(Artikel, Leserbrief etc.)
Redaktion Datenschleuder, Postfach 640236, D-10048 Berlin, Tel. +49 (30) 285.986.56 / *mailto:ds@ccc.de*

Druck

Pinguin-Druck, Berlin (*http://www.pinguindruck.de/*)

ViSdP

Tom Lazar, <tom@tomster.org>

Mitarbeiter dieser Ausgabe

Tom Lazar <tom>, Andy Müller-Maguhn <andy>, Jens Ohlig <jens>, Yannick <yannick>, Yinnick <yinnick>, Constantin Seibt <cs>, Christoph Rothe <redbaron>, Matthias Mehldau <wetter>, Carsten Wenzlow <knuckles>, Arne Ludorff <arne>, Dragan Espenschied <esp>, Alvar Freude <alvar>, The Artist <BGGFFICG>

Eigentumsvorbehalt

Diese Zeitschrift ist solange Eigentum des Absenders, bis sie dem Gefangenen persönlich ausgehändigt worden ist. Zur-Habe-Nahme ist keine persönliche Aushändigung im Sinne des Vorbehalts. Wird die Zeitschrift dem Gefangenen nicht ausgehändigt, so ist sie dem Absender mit dem Grund der Nichtaushändigung in Form eines rechtsmittelfähigen Bescheides zurückzusenden.

Copyright

Human Error

Your Name Brand Operating System and Browser, in conjunction with The Computer Industry, has determined that you have comitted a serious error. You will be permitted to continue on to the requested site on a temporary basis. The error described below must be corrected within 30 days to avoid undesired consequences.

The Computer Industry, after reviewing your purchasing history, has determined that you have failed to spend your prescribed minimum amount for new hardware and software. In order to better serve you, The Industry may, at it's sole option and without notice, terminate your computer, software, internet service, telephone service, cable connection, credit card, bank account, and life. Please assist us as we continue to work toward our Great New Future by obeying the instructions below. Failure to comply will force The Industry to escalate this incident to an Illegal Operation. Occasional extreme cases may require a Fatal Exception.

• Print this page, You will need it during later steps.

• Backup all your existing data. Be sure not to backup any software. User data will include your documents, photos, spread sheets, and E-mail. Please do not ask us how to do this. The Industry only tells you what is required of you, not how to do it.

• Next, place your computer, mouse, keyboard, monitor and all software in the trash. It is important that you do not allow anything to be reused, as this will violate many software licenses and interfere with The Industry's revenue growth.

• Check your favorite advertising sources for newly released computers and software. Please pay particular attention to release and availability dates. Select ONLY the very newest model of computer and the most recently released operating system. Purchase a new computer, operating system, and application software. Use credit if necessary.

• Restore the user created data you backed up in a previous step. Again, do not ask us how to do this. That is your responsibility.

• Repeat at least once every year.

Resistance is Futile

The Industry

The Artist <*theartist@art-techo.net*>

Aus dem Papierkörbchen einer Landesregierungsbehörde

"Sehr geehrte Kolleginnen und Kollegen, an allen PCs im [...] werden wir über das Landesverwaltungsnetz einen Internetzugang realisieren. Dieser Zugang muss aus Sicherheitsgründen und entsprechenden Vorgaben des Landesbeauftragten für Datenschutz auf die dienstlich notwendigen Internetseiten beschränkt werden.

"Wir bitten Sie, den IuK-Referat [1] [...] die von Ihnen benötigten Internetseiten zu benennen. (Bitte grundsätzlich die URL, also z.B. *http://www.baden-wuerttemberg.de* oder ausnahmsweise, falls nicht möglich, eine umgangssprachliche Beschreibung, die uns das Auffinden ermöglicht, zu benennen.)

Aus den gemeldeten Seiten werden wir dann das Gesamtangebot erstellen.

Mit freundlichen Grüßen [...]

Datenschutzbedenken gegen Payback - Rabattsystem werden vom Gericht bestätigt

Die Datenschutzaufsichtsbehörden der Länder Bremen, Berlin, Niedersachsen, Nordrhein-Westfalen und Schleswig-Holstein begrüßen die jetzt veröffentlichte Entscheidung des Landgerichts München I vom 1. Februar 2001 (Az.: 12 O 13009/00) - noch nicht rechtskräftig. Das Landgericht hat zwei Klauseln in den Anmeldeformularen des Payback-Rabattvereins e.V. auf Klage des Berliner Verbraucherschutzvereins beanstandet. Das Gericht hat in seinem Urteil dem Payback-Rabattverein verboten, die in den Antragsformularen enthaltenen zentralen Einwilligungsklauseln zur Datenverarbeitung zu verwenden oder sich auf diese Klauseln bei der Abwicklung derartiger Verträge zu berufen.

[1] Anm. d. Red.: Iuk = Information und Kommunikation

Das Gericht sieht in den Klauseln eine unangemessene Benachteiligung der Kundinnen und Kunden und erklärt die Einverständniserklärung betreffend die Verarbeitung und Nutzung der personenbezogenen Angaben gemäß § 9 Abs. 1 und Abs. 2 Nr. 1 AGB-Gesetz i.V.m. §§ 4 und 28 Bundesdatenschutzgesetz für unwirksam. Damit darf Payback die Daten seiner jetzigen Kundinnen und Kunden nur nach den Vorschriften des Bundesdatenschutzgesetzes verarbeiten, so weit dies zur Durchführung des Rabattverfahrens erforderlich ist. Vor rund einem Jahr ist das Rabattsystem "Payback" von einigen großen Firmen (real, Galeria-Kaufhof, DEA, Apollo, Consors, Europcar, AOL, dm-Drogerie Markt u.a.) eingeführt worden. Mittlerweile sind es über 20 Unternehmen, weitere sollen hinzukommen. Für die datenschutzrechtliche Prüfung ist die bayerische Datenschutzaufsichtsbehörde zuständig. Seit Einführung der Karte reißen die Nachfragen von besorgten Bürgerinnen und Bürgern und der Presse bei den Datenschutzaufsichtsbehörden nicht ab. Das liegt daran, dass weder die Einverständniserklärung noch die Allgemeinen Geschäftsbedingungen hinreichend deutlich machen wer über welche Daten verfügt und wo und von wem, welche Daten verarbeitet werden. Auch ist nicht klar: Werden die Daten über die gekauften Waren zusammen mit den personenbezogenen Daten der Kundinnen und Kunden für alle Zeit gespeichert und weiterverarbeitet? Welche Daten werden personenbezogen zwischen den Partnerunternehmen ausgetauscht? Was sind die in den Geschäftsbedingungen genannten Mailings , und welche personenbezogene Daten werden hierfür verarbeitet? Zweifel der Datenschutzaufsichtsbehörden werden nunmehr durch das Urteil gerichtlich bestätigt. Die unklare Einverständniserklärung, die die Kundinnen und Kunden abgeben müssen, entspricht nicht den Anforderungen des Bundesdatenschutzgesetzes (§ 4 Abs. 2 BDSG). Der Teilnehmer wird

nämlich weder eindeutig über Umfang und Zweck der Speicherung und die vorgesehene Datenübermittlung (welche Daten werden an Partnerunternehmen von Payback weitergegeben) hinreichend unterrichtet, noch wird den Kundinnen und Kunden eine hinreichende Möglichkeit eingeräumt, einzelne Datenverarbeitungsformen nicht zuzulassen. Was dem Kunden häufig nicht klar ist: Selbst bei Barzahlung wird er beim Kauf mit Rabattkarte eindeutig identifizierbar. Die Daten ermöglichen, das Kaufverhalten über mehrere Produktbereiche und Unternehmen hinweg personenbezogen auszuwerten. Aus der Verarbeitung persönlicher und kaufmännischer Daten kann zu jedem Teilnehmer ein Profil gebildet werden, das den Verbraucher zum gläsernen Kunden macht. Die Datenschutzaufsichtsbehörden erwarten nach dem Urteil nicht nur eine Korrektur der Anmeldeformulare, sondern eine klare Aufklärung der Kundinnen und Kunden, was mit ihren Daten in welchen Verarbeitungsphasen gemacht wird: Wenn das informationelle Selbstbestimmungsrecht gewahrt bleiben soll, müssen die Kundinnen und Kunden selbst entscheiden können, was mit ihren Daten geschieht. Wenn es den Unternehmen wirklich nur um die Kundenbindung geht, wie in den bunten Prospekten erklärt wird, sollte Payback wenigstens mit einer Variante seinen Kundinnen und Kunden ermöglichen, nur Rabattpunkte zu sammeln, ohne dass es zu einer weiteren Verarbeitung ihrer Daten zu anderen Zwecken kommt. Die Datenschutzaufsichtsbehörden werden die weitere Entwicklung auf diesem Gebiet der Kunden-/ Freundschafts-/ oder Rabatt - Kartensysteme, insbesondere nach Aufhebung des Rabattgesetzes, kritisch im Auge behalten. **<tom>**

Quelle: *http://*www.datenschutzzentrum.de

Ex-MI6 Agent veröffentlicht Memoiren im Internet

Richard Tomlinson hat nicht nur ein Buch über seine Tätigkeit beim Britischen Geheimdienst geschrieben, das als Abrechnung angesehen werden kann, sondern es auch kostenlos im Internet veröffentlicht. John le Carrés Romane sind zwar spannender, aber immerhin hat der MI6 mit allen Mitteln versucht, die Veröffentlichung dieses Buches zu verhindern... **<tom>**

Quelle: *http://*www.thebigbreach.com/download/

deCSS revisited...

Ganze sieben Zeilen perl braucht es mittlerweile nur, um das sowieso schon blamable 'Content Scrambling System' zu entschlüsseln mit dem die Motion Picture Association of America (MPAA) das Kopieren von DVDs verhindern wollte. Bevor deren Anwälte jetzt auch die Verbreitung dieses Codes durch Abmahnwellen unterbinden, schafft die Datenschleuder Fakten und druckt das kleine Meisterwerk einfach mal ab ;-)

```
#!/usr/bin/perl -w
# 531-byte qrpff-fast, Keith Winstein and Marc Horowitz
# <sipb-iap-dvd@mit.edu> MPEG 2 PS VOB file on stdin ->
# descrambled output on stdout
# arguments: title key bytes in least to most-significant order
$_='while(read+STDIN,$_,2048){$a=29;$b=73;$c=142;$t=25
5;@t=map{$_%16or$t^=$c^=($m=(11,10,116,100,11,122,20
,100)[$_/16%8])&110;$t^=(72,@z=(64,72,$a^=12*($_%16
-
2?0:$m&17)),$b^=$_%64?12:0,@z)[$_%8]}(16..271);if((@a=
unx"C*",$_)[20]&48){$h
=5;$_=unxb24,join"",@b=map{xB8,unxb8,chr($_^$a[--
$h+84])}@ARGV;s/...$/1$&/;$
d=unxV,xb25,$_;$e=256|(ord$b[4])<<9|ord$b[3];$d=$d>>8^(
$f=$t&($d>>12^$d>>4^
$d^$d/
8))<<17,$e=$e>>8^($t&($g=($q=$e>>14&7^$e)^$q*8^$q<
<6))<<9,$_=$t[$_]^
(($h>>=8)+=$f+(~$g&$t))for@a[128..$#a]}print+x"C*",@a}';
s/x/pack+/g;eval
```

Man sells his soul for $400 on E-bay

SEATTLE 2-9-01 (AP) E-bay has become the place to sell your soul. Adam Burtle, 20, sold his soul on the Internet auction site, fetching $400 before the listing was removed and the University of Washington student and part-time automotive technician was suspended from the site.

For his listing, the self-described atheist displayed a picture of himself wearing an "I'm with stupid" T-shirt.

"Please realize, I make no warranties as to the condition of the soul. As of now, it is near mint condition, with only minor scratches," he wrote. "Due to difficulties involved with removing my soul, the winning bidder will either have to settle for a night of yummy Thai food and cool indie flicks, or wait until my natural death."

EBay has blocked similar auctions in the past but said Burtle's soul slipped through.

The bidding started a week ago at 5 cents. Burtle's former girlfriend bid $6.66 but she was overtaken in the final hour of the auction on Thursday when the price shot up to $400.

The buyer was identified as a Des Moines, Iowa, woman with an eBay feedback rating of zero, meaning she has no track record with other users of the Web site.

"I don't think she's going to be able to collect on my soul, to be honest," Burtle said, adding he didn't intend for the ad to be taken seriously.

"I was just bored, and I'm a geek," Burtle said. "So anytime I'm bored, I go back to my Internet."

Das Quartalszitat:

Der Vorsitzende Richter am Landgericht Frankfurt, Heinrich Gehrke, der den Opec-Prozess geleitet und Fischer als Zeuge vernommen hatte, nannte die Ermittlungen "hochgradig lächerlich". Wenn die Staatsanwaltschaft "immer diese Maßstäbe anlegen würde, wäre sie zugemüllt mit Verfahren wegen Falschaussage", sagte Gehrke dem Sender n-tvb. Die Teile der Aussage Fischers, die zur Debatte stünden, hätten mit dem eigentlichen Prozess nicht das geringste zu tun gehabt, meinte der Richter. Vor deutschen Gerichten würde "von morgens bis abends gelogen". Die Folge der Ermittlungen sei, dass sich Zeugen künftig auf Errinerungslücken beriefen, wenn sie über Dinge befragt würden, die mehr als 30 Jahre zurücklägen. **<tom>**

Quelle: Handelsblatt 20.02.01

Staatssicherheit aufgelöst oder das Operationsgebiet eingenommen?

von Andy Müller-Maguhn

"Nach langer Verzögerung der Antwort leugnet die Bundesregierung nun weitgehendst die skandalösen Vorgänge, die mir während meiner USA-Reise unmißverständlich berichtet wurden: [...] daß die CIA derzeit mit tatkräftiger Unterstützung bundesdeutscher Dienste ehemalige Stasi-Offiziere unter Vertrag nimmt."
Aus einer Presseerklärung der innenpolitischen Sprecherin von Bündniss90/ Die Grünen vom 10.03.1992

Ergebniss einer bisher erst groben Analyse von Datenhinterlassenschaften

Manche Artikel basieren auf langen Geschichten. Bei anderen Artikeln ist es genau umgekehrt: Artikel verursachen lange Geschichten. Bei diesem Artikel ist die Geschichte evtl. in beide Richtungen gleich lang. Und zwar ziemlich.

Als die Deutsche Demokratische Republik (DDR) aufgelösst wurde, hat sie neben merkwürdigen Errinerungen auch noch - so glaubte man - einen der bestdokumentiertesten Geheimdienste der Welt hinterlassen. Die Gauck-Behörde, offziell "Der Bundesbeauftragte für die Unterlagen des Ministeriums für Staatssicherheit der ehemaligen Deutschen Demokratischen Republik" verwaltet immerhin etliche Tonnen Akten und macht sie den betroffenen - Tätern wie Opfern - mit gewissen datenschutzrechtlichen Einschränkungen zugänglich. Geschichtsaufarbeitung sollte möglich werden.

Die Bürger der ehemaligen DDR schienen erreicht zu haben was sie wollten: das Ministerium für Staatssicherheit (die "Stasi") war aufgelöst, die DDR auch, ein paar leitende Funktionäre im Gefängniss und die DDR jetzt BRD. Und jetzt kommen wir zu den Schönheistfehlern dieser Operation.

Bei der Auflösung des Ministeriums für Staatssicherheit wurden ja, wie das neudeutsch so schön heißt "einige Arbeitskräfte dem Markt freigestellt." Schon die Frage wieviele Mitarbeiter das Ministerium für Staatssicherheit denn hauptamtlich hatte, lässt sich leider nicht so einfach beantworten. Es gibt zwar einen Haufen Akten, und Personallisten, aber die Interpretationen dieses Materials gehen dann doch eher weit auseinander.

Nun war für die Bürger der ehemaligen DDR die Frage, wer denn nun früher für die Stasi gearbeitet hat oder nicht, schon eine Frage. Man wollte schließlich nicht mit den selben Genossen noch einmal die - vermeintlich - neuen Staatsstrukturen aufbauen. Hilfreich war u.a. die "Liste der Hauptamtlichen Mitarbeiter des MfS" die seit den frühen 90´er Jahren durch Publikationen der DDR-Bürgerbewegung verbreitet wurde. Sie enthält rund 100.000 Mitarbeiter bzw. Datensätze (genau: 97.058 plus minus ein paar) und gilt - präzise galt - als authentisch. Auch die juristischen Auseinandersetzungen die die Verbreiter dieser Liste bekamen (Neues Forum wegen Abdruck, Nie-

derspende.de wegen Verbreitung im Netz) sprachen zumindest dafür, daß die Liste echte Namen enthält.

Als die Bürgerbewegten die Daten in den frühen 90er Jahren mit dBase verarbeiten, waren die damals genutzten 386er eher an den Grenzen ihrer Belastung. Bei 100.000 Daten fielen komfortable Suchaktionen und Quervergleiche eher aus. Das ist zum Glück heute etwas anders.

Im Kontext eines Congresses in der ehemaligen Parteischule der Sozialistischen Einheitspartei Deutschlands (SED) der ehemaligen DDR kam neulich mal jemand vorbei und erzählt merkwürdige Geschichten: das ungefähr die Hälfte der Stasi-Mitarbeiter kurz vor der sogenannten Wiedervereinigung unter den Tisch gefallen sei. Zunächst war ein etwas toleranter Umgang mit dem Fassungsvermögen der eigenen Hirnstrukturen gefordert: die Mauscheleien zwischen Ost- und Westdiensten, die der junge Mann skizzierte waren zwar in sich schlüssig, entbehrten allerdings auch nicht einer gewissen Komplexität. Nachweise sollten folgen.

Ein Hinweis war, daß mit der erwähnten Mitarbeiterliste der Hauptamtlichen Mitarbeiter etwas nicht stimmte; bestimmte Geburtstage wurden in Ihnen fehlen. Und damit fängt die Geschichte an, auch wenn dieser Artikel nur eine erste Auflistung von Merkwürdigkeiten liefern kann.

Die Mitarbeiterliste der Hauptamtlichen Mitarbeiter ist im Netz verfügbar: mit dem Dateinamen ma_stasi.zip wird man z.B. fündig. Welche Version ihr allerdings im Netz findet, die von welcher Dienststelle welchen Geheimdienstes modifiziert wurde, kann ich euch nicht sagen. Als Orientierung kann http://cryptome.org/stasi-list.htm helfen.

Die Struktur dieser Datenbank bzw. Liste besteht aus:

• Personenkennzeichen (PKZ)

Das PKZ ist das Identifikationskennzeichen für DDR-Bürger. Setzt sich zusammen aus Geburtsdatum (TTMMJJ), Geschlechtskennzeichen (4=m 5=w), 4 stelliger Ursprungskennziffer (erste Anmeldung) und einer Prüfziffer. Algorithmus liegt vor. Datenbank der Ursprungskennziffer ist derzeit noch in der Erstellung (schlecht lesbare Papiervorlage). Die Papiere gibt es in Kürze auf ftp://ftp.ccc.de/pub/infopool/mfs/

• Einheitenschlüssel (AB;CD;EF)

Der Einheitenschlüssel besteht aus 3 Gruppen á zwei Nummern, wird aber zusammengezogen interpretiert. Er gibt die Einheit des MFS an, bei dem der/diejenige gearbeitet hat. Strukturdatenbank ist auf ftp://ftp.ccc.de/pub/infopool/mfs/einheiten.dbf (bzw. .txt, .tab, .fm)

• Namensfeld (Name, Vorname)

• Gehalt

Die genaue Bedeutung des Gehaltsfeldes ist umstritten. Einige Behaupten, es handele sich hier um das Jahresgehalt. Andere sagen, es sei das Gehalt seit Frühjahr 1989. Dritte sagen was ganz anderes. Klar ist: die Liste enthält Gehaltszahlen aus denen sich möglicherweise ein Hierarchiestatus inter- pretieren lässt. Das kann Information oder Desinformation sein.

Zunächst sind wir also dem Hinweis auf Unregelmässigkeiten im Bezug auf die Geburtsdaten nachgegangen. In der Tat scheint es bei der Stasi gewisse Geburtsschwache Tage gegeben zu haben; unabhängig vom Geburtsjahr der jeweiligen finden sich weder am 17.03., 17.04., 17.05., 17.06., 17.07., 17.08. irgendwelche Einträge. Am 17.02. finden sich zwar 2 Einträge, allerdings sind beide aus dem Jahrgang 1927. Bei allem Verständniss für historische Aufarbeitung handelt es sich hier offensichtlich um Rentner.

Alle anderen Geburtstage scheinen in der Datenbank sehr gleichmässig verteilt zu sein. Bei einer groben Annahme (Sollwert) von 100.000 Einträgen, geteilt durch die Anzahl möglicher Geburtstage (365) wäre der mathematische Richtwert 273 Geburten pro Tag. In Unkenntnis etwaiger Geburtenschwachen Tagen bzw. Monaten handelt es sich bei den vorliegenden Zahlen entweder um eine erstaunlich primitiv frisierte Datenbase oder um eine relativ mittelwertgenaue Geburtsanhäufung.

Diese beiden Indikatoren (fehlende 17. und Mittelwert-Genauigkeit) können insofern nur bedingt als Indizen für eine Datenmanipulation gewertet werden. Für beide sind "natürliche" Erklärungen dankbar. Im Bezug auf die fehlenden Geburten an den 17. kann es sich um einen - immerhin 10 Jahr nicht bemerkten - Datenverlust bei der Konvertierung von Datenträgern schlechter Qualität handeln. Ein entsprechender Hinweis auf mögliche Datenträgerschäden liegt aus den Kreisen der konvertierenden Bürgerbewegten vor, konnte allerdings bis Redaktionsschluss noch nicht verifiziert werden. Ob der Indikator der "gleichmässigen" Verteilung (die Geburten pro Tag bewegen sich alle passgenau um den Mittelwert von 273) gewertet werden kann, kann ich mangels Hinweisen auf etwaige übliche ungleichmässigen Verteilungen nicht feststellen.

Wesentlich aufschlussreicher und als deutlichster Hinweis kann da schon der Abgleich der vorhandenen Datensätze der Hauptamtlichen Mitarbeiter mit dem Einheitenschlüssel gelten. Von den 2286 insgesamt vorhandenen Abteilungen der Staatssicherheit wären beispielsweise 1349 ohne einen einzigen Mitarbeiter. Diese Unterbesetzung ist wohl selbst bei großzügiger Lesart unrealistisch.

Noch deutlicher wird die Manipulation der HA-Datenbank allerdings, wenn man sich die Einheitenzuweisung im Detail anguckt. Als Beispiel für eine etwas detailliertere Analyse sei hier mal die Hauptabteilung III (Funkaufklärung) genommen. Unter dem "generellen" Einheitenschlüssel 940300 finden sich immerhin insgesamt 2312 Mitarbeiter. In den jeweiligen Diensteinheiten finden sich allerdings keine Mitarbeiter. Eine grobe Hierarchie ließe sich zwar aus den Gehaltszahlungen ableiten, aber keine Zuweisung zu den Diensteinheiten.

Schlüssel	Oberbereich	Unterbereich	Diensteinheit	Anzahl MA
940300	Zentralbereich	Hauptabteilung III Funk / Technik		2312
940301	Zentralbereich	Hauptabteilung III Funk / Technik	Leiter	0
940302	Zentralbereich	Hauptabteilung III Funk / Technik	1. Stellvertreter des Leiters	0
940303	Zentralbereich	Hauptabteilung III Funk / Technik	Stellvertreter des Leiters	0
940304	Zentralbereich	Hauptabteilung III Funk / Technik	Stellvertreter des Leiters	0
940305	Zentralbereich	Hauptabteilung III Funk / Technik	Stellvertreter des Leiters	0
940309	Zentralbereich	Hauptabteilung III Funk / Technik	Stellvertreter des Leiters	0
940306	Zentralbereich	Hauptabteilung III Funk / Technik	Bereichsleiter	0
940307	Zentralbereich	Hauptabteilung III Funk / Technik	Bereichsleiter	0
940308	Zentralbereich	Hauptabteilung III Funk / Technik	Bereichsleiter	0
940311	Zentralbereich	Hauptabteilung III Funk / Technik	Sekretariat	0
940312	Zentralbereich	Hauptabteilung III Funk / Technik	AKG	0
940313	Zentralbereich	Hauptabteilung III Funk / Technik	AG des Leiters	0
940315	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 3	0
940316	Zentralbereich	Hauptabteilung III Funk / Technik	AG Finanzen	0
940319	Zentralbereich	Hauptabteilung III Funk / Technik	PO-Leitung	0
940322	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 11	0
940324	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 4	0
940325	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 5	0
940326	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 1	0
940327	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 2	0
940328	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung VO	0
940331	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 6	0
940332	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 7	0
940333	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 8	0
940334	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 9	0
940335	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 10	0
940336	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 12	0
940337	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 16	0
940338	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 13	0
940339	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung 14	0
940341	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung TN	0
940342	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung T2	0
940343	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung T3	0
940344	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung T4	0
940345	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung T6	0
940346	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung T1	0
940347	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung T5	0
940351	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung F1	0
940352	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung F2	0
940353	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung F3	0
940354	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung F4	0
940381	Zentralbereich	Hauptabteilung III Funk / Technik	Abteilung Planung	0

Diese Strukturverschleierung tritt bei allen Hauptabteilungen auf, in den Bezirksverwaltungen des MfS hingegen ist sie vorhanden. Wenn die Strukturverschleierung in der Datenbank eine grundsätzlich vom MfS betriebene wäre, würde sie wohl kaum die Bezirksverwaltungen außen vor lassen. Als Beispiel hierfür sei willkürlich Leipzig gewählt.

Schlüssel	Oberbereich	Unterbereich	Diensteinheit	Anzahl HA
130000	BV Leipzig	Kreis- und Objektdienststellen	KD-Namen fehlen	0
139901	BV Leipzig	Leitungsebene	Leiter	7
139902	BV Leipzig	Leitungsebene	1. Leiter-Stellv.(Operativ)	0
139903	BV Leipzig	Leitungsebene	Stellvertreter Operativ	0
139904	BV Leipzig	Leitungsebene	Stellv. für Aufklärung/Leiter	0
139905	BV Leipzig	Leitungsebene	Stellvertreter OT	0
139906	BV Leipzig	Leitungsebene	AG Aktionen und Einsätze	8
139910	BV Leipzig	Leitungsebene	persönlicher Referent des	0
130100	BV Leipzig	selbständi. Referat Abwehr WBK		5
130200	BV Leipzig	Abteilung II		56
130300	BV Leipzig	Abteilung III		26
130600	BV Leipzig	Abteilung VI		57
130700	BV Leipzig	Abteilung VII		27
130800	BV Leipzig	Abteilung VIII		146
130900	BV Leipzig	Abteilung IX		46
131100	BV Leipzig	Abteilung XI		18
131200	BV Leipzig	Abteilung XII		30
131400	BV Leipzig	Abteilung XIV		52
131500	BV Leipzig	Abteilung XV		48
131800	BV Leipzig	Abteilung XVIII		99
131900	BV Leipzig	Abteilung XIX		43
132000	BV Leipzig	Abteilung XX		93
132200	BV Leipzig	AG XXII		6
132600	BV Leipzig	Abteilung 26		48
132900	BV Leipzig	BKG		16
133000	BV Leipzig	Abteilung OT		15
134000	BV Leipzig	Abt. Kader und Schulung		61
134100	BV Leipzig	PO-Leitung		7
139000	BV Leipzig	BV der Volkspolizei	BdVP Leipzig	0
139100	BV Leipzig	BV Zoll	Zoll-Bezirksverwaltung	0
139900	BV Leipzig	Leitungsebene		0
130040	BV Leipzig	Kreis- und Objektdienststellen	KD-Namen fehlen	187
130041	BV Leipzig	Kreis- und Objektdienststellen	KD-Namen fehlen	77
130042	BV Leipzig	Kreis- und Objektdienststellen	KD-Namen fehlen	61
130043	BV Leipzig	Kreis- und Objektdienststellen	KD-Namen fehlen	75
130044	BV Leipzig	Kreis- und Objektdienststellen	KD-Namen fehlen	37
130045	BV Leipzig	Kreis- und Objektdienststellen	KD-Namen fehlen	51
130046	BV Leipzig	Kreis- und Objektdienststellen	KD-Namen fehlen	40
130047	BV Leipzig	Kreis- und Objektdienststellen	KD-Namen fehlen	28
130048	BV Leipzig	Kreis- und Objektdienststellen	KD-Namen fehlen	36
130049	BV Leipzig	Kreis- und Objektdienststellen	KD-Namen fehlen	33
130050	BV Leipzig	Kreis- und Objektdienststellen	KD-Namen fehlen	26
130051	BV Leipzig	Kreis- und Objektdienststellen	KD-Namen fehlen	38

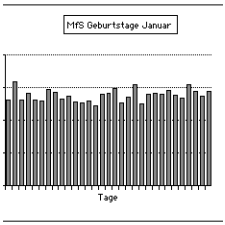
Hier allerdings liegen die Unterabteilungen offen; lediglich auf der Ebene der Leiter fehlen die Hinweise. Und dann gibt es noch Mitarbeiter in Abteilungen, wo nur die Abteilungsschlüssel vorliegen, allerdings nichts über die Abteilungen selbst bekannt ist.

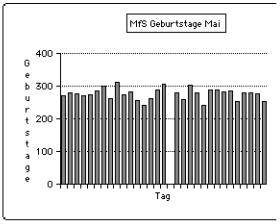
Als Zusammenfassung dieser ersten groben Analyse muss man wohl feststellen, daß aufgrund dieser deutlichen Indikatoren für eine Manipulation der Datenbestände auch die anderen Abteilungszuweisungen nicht wirklich als verlässliche Werte angenommen werden können. In Zusammenhang mit verschiedenen Hinweisen auf den Zeitraum, der der Staatssicherheit für eine Strukturverschleierung bzw. partielle Verlagerung von Personalbeständen in andere Organisationen (Wirtschaftsunternehmen, staatliche geführte Unternehmungen etc.) zur Verfügung stand, könnnte man sich schon sorgen machen. Wenn man dann noch die Hinweise auf die Übernahme des kompletten Personalbestands einzelnder Abteilungen durch andere Dienste - z.B. amerikanische - hinzuzieht, kann man sich wahlweise in schlechter Laune oder Aufdeckung aktiver Strukturen üben.

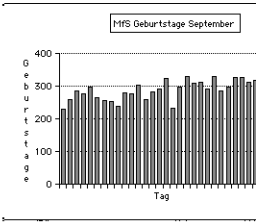
Um eine gründlichere Analyse durchzuführen, gibt es zunächst verschiedene Gedankenspiele. Die meisten Forschungsanträge der Gauck-Behörde und verfügbare Literatur über die Aktivitäten des MfS betreffen beispielsweise eher Thematische als Strukturelle Belange. Eine systematische Struktur- analyse wäre also in den jeweiligen Bereichen ein möglicher Ansatz.

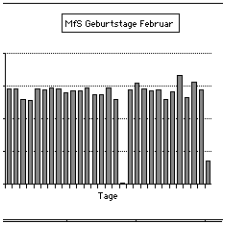
Weitere mögliche Herangehensweisen wären durch differenzierte Arbeitshypothesen denkbar. Wenn man beispielsweise die offensichtliche Datenmanipulation der Hauptamtlichen Liste zusammen mit den Rentenansprüchen ehemaliger HA´ler in die These der gewinnträchtigen Einführung von Personen mit mehreren Identitäten umwandelt, gäbe dies Anlass zur Überprüfung gewisser Geburtstage. Viel Spaß am Gerät.

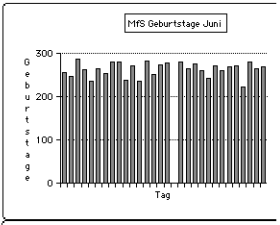
Wer noch Material beizusteuern hat, ist herzlich eingeladen, dies an die Redaktion Datenschleuder auf elektronischem (ds@ccc.de) oder postalischem Wege (Postfach 640236, D-10048 Berlin) zu tun.

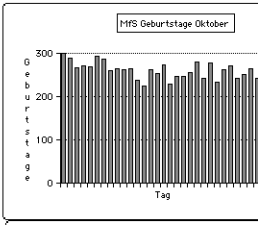


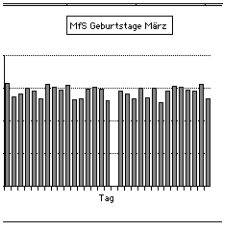


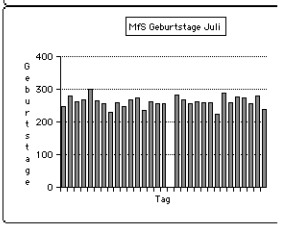


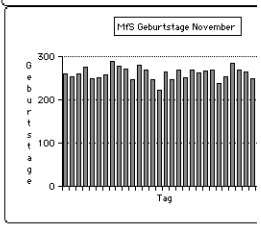


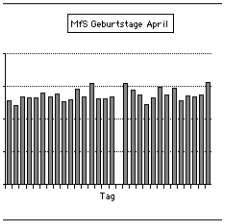


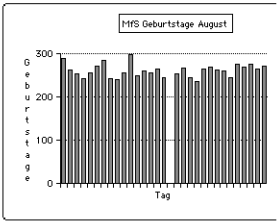


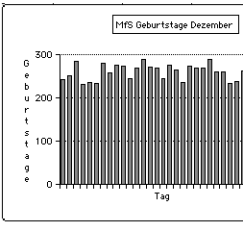












	A	B	C	D	E	F	G	H	I	J	K	L
1	261	292	316	255	271	256	246	288	228	299	259	242
2	319	292	275	240	279	247	280	263	258	289	254	251
3	263	260	281	267	277	286	262	254	284	266	261	285
4	282	255	299	264	271	262	267	242	276	271	276	231
5	263	292	291	265	273	235	301	256	298	269	250	236
6	258	288	269	278	284	265	264	271	264	294	251	233
7	293	295	313	268	301	254	257	284	255	286	258	280
8	284	291	303	276	263	281	228	243	252	261	290	257
9	264	280	293	253	312	279	258	241	238	265	278	275
10	275	285	308	258	273	237	248	255	280	262	271	273
11	255	285	266	290	282	272	269	298	277	264	247	244
12	253	293	268	268	256	236	274	248	303	237	281	268
13	259	275	296	310	242	283	236	260	260	225	270	289
14	245	273	303	261	261	252	261	256	281	263	246	271
15	279	294	296	262	288	273	256	265	292	254	223	270
16	281	259	262	267	307	277	257	245	325	273	265	245
17	297	2	0	0	0	0	0	0	233	229	246	275
18	253	289	292	309	280	281	282	254	297	18	270	264
19	270	308	282	288	259	264	268	267	328	247	251	236
20	309	291	269	273	303	275	255	245	310	255	270	274
21	250	286	299	245	279	260	263	236	311	279	263	268

SecurEdoc bei TNT: Ein kleiner, feiner Hack und ein mittlerer Datenschutzskandal

von Jens Ohlig und Yannick und Yinnick

Hacken ist manchmal ganz einfach: Es reicht eine dünne Leitung und ein handelsüblicher Browser, man braucht weder crack noch portscan. Bei TNT SecureEdoc konnten mit solchen Mitteln private Daten anderer betrachtet werden, sofern man denn im Geheimwissen der mathematischen Grundrechenarten bewandert ist.

TNT SecureEdoc [1] ist ein bezahlter Dokumentenaustauschdienst des international bekannten Paket- und Logistikservice TNT, programmiert wurde diese Anwendung vom amerikanischen Softwareunternehmen Certia [2]. Mit diesem Angebot will sich TNT offenbar auf dem Markt als Logistikdienstleister platzieren, der auch im Online-Bereich den Austausch von Dokumenten sicher abwickelt. Dabei setzt man auf eine Datenbank, in der die ausgetauschten Daten abgelegt werden. Der Schlüssel zu den Nachrichten ist die Package-ID, die -- wie später erklärt -- einfach auszurechenen ist. Dabei ist der Dienst nicht nur für den Austausch zwischen zwei angemeldeten Nutzern gedacht, sondern auch mit Usern, die keinen Account haben, aber trotzdem eine von einem eingetragenen und zahlenden TNT-Kunden Dokumente erhalten sollen. Dazu wird der vom Nutzer angegebenen Email-Addresse eine Nachricht mit der Package-ID gesendet. Doch das an sich schon sträfliche Loch der Abhörbarkeit von SMTP- und POP-Verbindungen auf dem Weg durch das Netz wird noch übertroffen von der Vorhersagbarkeit der übermittelten Package-ID.

[1] http://www.tnt-securedoc.com
[2] http://www.certia.com/

Zum Betrachten der Nachricht muß der Empfänger die URL, die u.a. die Package-ID enthält, einfach in seinem Browser öffnen. Nach dem einfachen Klick erschien sofort die Seite mit der auzutauschenden Nachricht. Restriktion an der Stelle ist nur, ob diese Nachricht nicht nur auf den Status "nur ein mal lesbar" gesetzt wurde -- ein ohnehin zweifelhaftes Feature bei manch "hängender" Leitung. Die letzten Ziffern der Package-ID sind zweigeteilt: Die erste Kolonne bezeichnet den Empfänger und die zweite die Dokumenten-Nummer. D.h. durch einfaches Subtrahieren von Werten von diesen Nummern konnte man die Nachrichten anderer Nutzer sehen.

Dabei war natürlich nicht jede beliebige Kombination gültig. Wurden mehrere Dokumente gleichzeitig verschickt, wurde die zweite Hälfte der Package-ID um die Anzahl der verschickten Dokumente verringert, wurde die Nachricht an mehrere Empfänger verschickt, wurde wurde die erste Hälfte der Package-ID um diese Anzahl verringert. Die Anzahl der Dokumente und Empfänger konnte man in der angezeigten Nachricht erkennen und wußte -- mit wenig Kopfrechnen -- sofort, welches die Package-ID des vorhergehenden Vorganges war. Weiter wäre es möglich gewesen, mit ein wenig Par-

sen und Cookie-Verwaltung der HTML-Dateien ein Skript ans laufen zu bekommen, daß die Zahl der Dokumente und Empfänger jeweils ausliest und automatisch Nachricht für Nachricht einliest und verarbeitet.

Um durch dieses Vorgehen sukzessive die anderen Nachrichten zu öffnen brauchte man also nur eine Ankernachricht mit Ausgangszahlen; glücklicherweise kann man sich zum Testen eintragen und somit Nachrichten an einen Account schicken, auf den man selber Zugriff hat. Da dies ein bezahlter Dienst ist, kommt einem auch die Bezahlung per (Online-)Rechnung entgegen, es ist aber in dem Dienst auch möglich, die Beträge per Kreditkarte zu bezahlen. Und spätestens da wird es richtig unangenehm für die Nutzer: Da der Dienst ja speziell für den Austausch sensibler Daten geschaffen wurde, liegen auch die Bestätigungen der persönlichen Daten inklusive der Kreditkartendaten als Nachrichten im System vor. Bingo!

Die Kreditkartendaten waren noch das Interessanteste, was in dem System gefunden werden konnte. Daneben lagen dort Bilanzen, Unterlagen zur Steuer, Kundentabellen etc. Da dieser kostenpflichtige Dienst besonders damit warb, vertrauliche Daten auf sicherem Weg auszutauschen, waren die dort vorzufindenden Inhalte zum großen Teil solcher Natur. Zum Vergleich: Selbst bei unverschlüsselter Email, die leicht mitgelesen werden kann, sind die Daten, einmal beim Empfänger angekommen, nicht mehr potentiellen Angreifern ausgesetzt.

Nachdem in den Kölner Räumlichkeiten des CCC diese Schwachstellen ausgelotet wurden, haben wir zunächst TNT als Betreiber des Dienstes informiert. Schließlich wurden hier private Daten von Benutzern des Systems der Öffentlichkeit zur Verfügung gestellt. Musste ja nicht sein. Schwieriger war es, einen Ansprechpartner zu finden, der einzige erfolgsversprechende Anruf erfolgte dann schliesslich beim Pressesprecher der deutschen Niederlassung. Man tat eifrig ("Ja, was für ein Computerclub war das noch mal?"), aber nach einer Woche gab es dann immer noch keine Rückmeldung. Na gut, dann war man bei TNT wohl daran interessiert, das ganze über dpa zu erfahren. Und so geschah es dann auch. Nach der Veröffentlichung der Pressemitteilung wurde der Dienst nach weiteren 24 Stunden ausgesetzt. Nach einer Woche wird jetzt eine weitere Abfrage eines zusätzlichen Authentifizierungs-Tokens vorgenommen, bevor die Nachrichten abrufbar sind. Die Problematik des Abhorchens der Maildaten löst das aber auch noch nicht.

Bei TNT ist einem die ganze Sache wohl eher peinlich. Hinter vorgehaltener Hand gab ein Mitarbeiter von TNT Deutschland zu, dass der Service ja auch eher mit der heissen Nadel gestrickt worden war: "Ich meine, wer braucht so einen Scheiss?" Certia, die weiterhin auf ihren Webseiten mit dem zweifelshaften Slogan *"Bringing trust and control to a digital world"* wirbt, hatten in der Zwischenzeit ebenfalls Kontakt mit dem CCC aufgenommen. Ja, man sei an einem Gespräch interessiert. Der weitere Mailverkehr gestaltete sich allerdings als sehr schleppend, so dass bis heute kein Termin gefunden wurde. Interessant mag die Anschrift von Certia sein: Die "Sicherheitsfirma" ist in Virgina untergebracht, wo auch die Drei-Buchstaben-Organisationen der USA sich heimisch fühlen. Gerade in Herndon, wo Certia seinen Sitz hat, gibt es wohl auch mehrere Projekte von einer Organisation mit einem Namen, der dem von Certia verdächtigt ähnelt: Einfach die Buchstaben E, R und T wegnehmen. Man kann in diesem Zusammenhang paranoid werden, muss es aber nicht. Es könnte alles nur ein Beispiel für besondere Dummheit in der Softwareentwicklung gewesen sein, über das der CCC hier gestolpert ist. Vielleicht lebt es sich mit dieser Theorie angenehmer, wohliger, zufriedener. Vertrauen und Kontrolle in einer digitalen Welt.

Dummheit - ein grausamer, globaler Gott

von Constantin Seibt

Selten, aber doch passieren völlig unerwartete Dinge. Manchmal verliert Goliath tatsächlich gegen David. Manchmal tut Dummheit tatsächlich weh. Manchmal ist das Resultat eines Justizaktes tatsächlich Gerechtigkeit.

Die erstaunliche Geschichte begann mit einer typischen Freitagsverhaftung. Der Genfer Untersuchungsrichter Marc Tappolet stürmte in Begleitung von Berner und Genfer Polizisten in eine Berner WG, beschlagnahmte die Computer und überführte einen zwanzigjährigen Informatikspezialisten namens David ins Untersuchungsgefängnis nach Genf. In einem von keiner Unschuldsvermutung getrübten Communiqué gab Richter Tappolet bekannt: «Heute Morgen ist einer der Täter festgenommen worden.»

Dem Verhafteten - angeblich einer der Wef-Hacker - wurde Eindringen in ein Datenverarbeitungssystem, Sachbeschädigung sowie Scheck- und Kreditkartenbetrug vorgeworfen. Darauf steht eine Haftstrafe von bis zu fünf Jahren. Es ging um einen der spektakulärsten Coups in der an Coups nicht armen Hacker-Geschichte. Ein Kollektiv namens «Virtual Monkeywrench» hatte den Server des Weltwirtschaftsforums geknackt und der Presse eine CD mit E-Mail-Adressen, Passwörtern, Telefon- und Kreditkartennummern zugestellt: eine gigantische Kartei von 102 000 VIPs, darunter Clinton, Arafat und abertausende von Wirtschaftsbossen. Das Wochenende nach der Verhaftung brachte zunächst wenig Neues. Die Medien schrieben Kurzmeldungen, die Anti-WTO-Koordination verlangte die Freilassung des Gefangenen, das Wef schwieg, der Untersuchungsrichter blieb wie vom Erdboden verschluckt, der Verhaftete schmorte drei Tage im Kunstlicht seiner Zelle - der tiefere Sinn jeder Freitagsverhaftung. Allerdings ging die Rechnung der Strafverfolger nicht auf: Er schwieg.

Erst am Montag bekam der Anwalt Jean-Pierre Garbade die Akten und den Angeklagten zu sehen: «Eine sehr sympathische Person, von der ich viel über Informatik gelernt habe.» Auch wenn die Gegenseite die Lektionen nötiger gehabt hätte: Denn die Verhaftung seines Mandanten sei «nur durch völlige Unkenntnis in Computerdingen» erklärbar - ausser vielleicht aus dem «Wunsch heraus, die Tatsachen zusammenzubiegen». (Der Angeklagte - Informatiker, also offensichtlich hackkompetent und überdies politisch bei der anarchistisch orientierten Gewerkschaftsgruppe FAUCH tätig - passte bestens in das Fahndungsbild.) Die mitgelieferten Akten hingegen erwiesen sich als einzige Bombe. 1. Der Experte des Untersuchungsrichters ist selbst der grösste Entlastungszeuge. 2. Seine Aussage ist pures Dynamit gegen den Kläger: Er überführt das zigmillionenschwere Wef einer geradezu fahrlässigen Amateurhaftigkeit - und das auf dessen Kerngebieten Sicherheit, Diskretion und Hightech. Jedenfalls wurde nun zum ersten Mal klar, wie der Wef-Hack im Detail lief.

Das von der «SonntagsZeitung» interviewte Hacker-Kollektiv hatte nicht im Mindesten untertrieben, als es behauptete, ihre Tat sei im Grunde «weder ein Hack, noch ein Crack» gewesen, sondern «das Spazieren in einen

offenen Hof». Tatsächlich lagen die mit Quickbase angelegten Wef-Datenbanken so offen da wie möglich. Während in Davos die VIPs mit dem grössten Polizeiaufgebot seit dem Weltkrieg geschützt wurden, lagerten in Cologny ihre Daten so sicher wie ein Nichtschwimmer in einem Haifischbecken. Der erste und kleinste Fehler war ein Sicherheitsloch in einem, so der Genfer Experte, «miserabel konfigurierten System». Das Loch trug den Namen Port 1433 - eines von ein paar tausend Ports, mit dem der Server mit der Aussenwelt kommuniziert. (Benutzt werden normalerweise nur ein Dutzend - für Netze, Mails etc. - während der Rest geschlossen zu sein hat.) Der Zustand der Ports lässt sich mit Software aus dem Internet problemlos scannen - eine Routinesache von wenigen Minuten, zu der es minimale Informatikkenntnisse braucht. Ebenso banale Routine ist, bei einem offenen Port herauszufinden, was für ein System sich dahinter verbirgt: Im Falle des Wef war es ein Microsoft-Server mit dem Betriebssystem Windows 2000.

Der Fehler hatte aber für einmal nichts mit Microsoft zu tun: DENN SIE ÄNDERTEN DAS STANDARD-PASSWORT DER DATENBANK NICHT. Jede frisch gelieferte Microsoft-Quickbase-Datenbank räumt dem Benutzer beim ersten Aufschalten mit dem Benutzernamen «sa» und dem Passwort «» (Returntaste) die Rechte eines Systemadministrators ein. Dies zu ändern, passiert normalerweise am ersten Tag - beim Wef passierte es nie. Nun also hatten die Hacker den vollen Zugang zum Server des Wef. Das wäre peinlich genug gewesen, aber mehr Schaden als gelesene E-Mails oder die mit Anti-Wef-Parolen übermalten Sites des Forums wäre nicht dringelegen. Aber das Wef machte noch einen dritten unglaublichen Fehler: Irgendwann im Jahr 2000 hatte es weite Teile der vertraulichen Datenbank VON SEINEM INTERNEN AUF DEN WEB-SERVER KOPIERT. (Was ungefähr so fahrlässig ist, als würde man den Familienschmuck im draussen montierten Briefkasten aufbewahren.) Dass der interne Server und der immer gefährdete Web-Server physisch getrennt sind, gehört zum kleinen Einmaleins jedes Netzwerkadministrators.

Die von der WoZ befragten Experten zeigten sich gleichermassen amüsiert und entsetzt. «Suboptimal», urteilte der Datenbankarchitekt Alain Stamberger trocken und weigerte sich, weitere Äusserungen zitieren zu lassen, weil «diese dann beleidigend» wären - klar sei jedenfalls, dass die Aussage des Wef-Pressesprechers Charles McLean «Unser IT-Sicherheitsstandard ist auf höchstem Niveau» so zutreffend sei wie [zensiert]. Als «unglaublich, quasi eine Einladung, als würde man eine Luxuslimousine mit steckendem Zündschlüssel in einer dunklen Gasse abstellen», beurteilte der Pressesprecher Jens Ohlig des Hamburger Chaos Computer Clubs den Wef-Sicherheitsstandard. Die Wef-Hacker hätten durchaus «mit etwas krimineller Energie eine fast unbegrenzte Menge Schaden» anrichten können. Dass sie den Fall nur per Medien publik machten, sei das Minimum an Strafe gewesen. Eigentlich müsse das Wef danken: «Es war eine kostenlose Überprüfung eines sehr eklatanten Sicherheitslochs.» So weit zum glimpflich davongekommenen Goliath. Was den verhafteten David angeht, so stehen seine Chancen laut seinem Anwalt bestens. Nachgewiesen werden kann ihm nur das Scannen der Ports von seinem eigenen Computer aus - eine Sache, die so strafbar ist wie das Anklopfen an eine Tür. Der Expertenbericht des Untersuchungsrichters hält klar fest, dass im Log-File der Wef-Firewalls nur Aufzeichnungen über die Scans, aber nichts über das erfolgreiche Eindringen in Port 1433 existierte. (Eine Firewall, die das Klingeln an der Tür registriert, den Einbruch aber nicht.)

Kurz: Da Port 1433 monatelang offen stand, könnte die halbe Welt Anfang Januar im Wef

gewesen sein. Hält Untersuchungsrichter Tappolet nicht noch einen Trumpf im Ärmel, ist sein Bluff zu Ende. Klar ist jedenfalls, dass durch die Verhaftung von David die wahre Natur Goliaths enthüllt wurde: Das hochtechnisierte, hochexklusive, hochabgeschottete World Economic Forum, zuständig für die globale Elite und die Verbesserung der Welt, wird seinerseits von einer global wirkenden Kraft regiert: der grenzenlosen Dummheit. [1]

Offtopic

A wealthy man decided to go on a safari in Africa. He took his faithful pet dog along for company. One day the dog starts chasing butterflies and before long he discovers that he is lost. So, wandering about he notices a leopard heading rapidly in his direction with the obvious intention of having lunch.

The dog thinks, "Boyo, I'm in deep doodoo now."(He was an Irish setter).... Then he noticed some bones on the ground close by, and immediately settles down to chew on the bones with his back to the approaching cat.

Just as the leopard is about to leap, the dog exclaims loudly, "Man, That was one delicious leopard. I wonder if there are any more around here?" Hearing this the leopard halts his attack in mid stride, as a look of terror comes over him, and slinks away into the trees.

"Whew", says the leopard." That was close. That dog nearly had me."

Meanwhile, a monkey who had been watching the whole scene from a nearby tree, figures he can put his knowledge to good use and trade it for protection from the leopard. So, off he goes. But the dog saw him heading after the leopard with great speed, and figured that something must be up.

The monkey soon catches up with the leopard, spills the beans and strikes a deal for himself with the leopard. The cat is furious at being made a fool of and says, "Here monkey, hop on my back and see what's going to happen to that conniving canine. "

Now the dog sees the leopard coming with the monkey on his back, and thinks," What am I going to do now?" But instead of running, the dog sits down with his back to his attackers pretending he hasn't seen them yet.

And just when they get close enough to hear, the dog says, "Where's that monkey. I just can never trust him. I sent him off half an hour ago to bring me another leopard, and he's still not back!!"

[1] Dieser Artikel erschien ursprünglich in der Wochenzeitung Schweiz, 28.02.2001. Besten Dank für die Abdruckgenehmigung an den Autor ;-)

Virtuelles Datenschutzbüro gegründet

von Christoph Rothe

Anfang Dezember entstand das virtuelle Datenschutzbüro. Was es damit auf sich hat fragten wir Marit Köhntopp vom Datenschutzzemtrum Schleswig-Holstein.

DS: Was sind die Schwerpunkte des virtuellen Datenschutzbüros ?

MK: Die Schwerpunkte des virtuellen Datenschutzbüros sind: - Ansprechstelle im Internet für Datenschutzfragen von Nutzerinnen und Nutzern als Service von Datenschutzinstitutionen aus aller Welt - Informationen rund um Datenschutz - Diskussionsforen zu aktuellen Datenschutzthemen - Plattform für die Zusammenarbeit mit Datenschützern Die Arbeitsweise orientiert sich an der Open-Source-Tradition, d.h.: - offene Diskussionen - Entwickeln und Bereitstellen frei verfügbarer Privacy-Tools - Transparenz der Konzepte - JedeR kann mitmachen.

Die Ziele: - eine bessere Qualität des Datenschutzes, - durch Arbeitsteilung und Kooperation effiziente Nutzung aller vorhandenen Ressourcen, - Fortschreiben des Stands der Technik in Richtung "Privacy-Enhancing Technologies".

DS: Wer ist bereits an diesem Projekt beteiligt ?

MT: Die jetzigen Projektpartner finden sich unter: http://www.datenschutz.de/partner/ Weitere haben ihre Teilnahme angekündigt und werden in Kürze hinzustossen.

DS: Wer kann sich an diesem Projekt beteiligen und wodurch ?

MT: JedeR kann sich beteiligen: - Nutzerinnen und Nutzer, indem sie reinschauen, sich informieren und mitdiskutieren (insbesondere auf Mailinglists) - Expertinnen und Experten, indem sie ihre Beiträge einbringen und mitdiskutieren - Datenschutzinstitutionen, indem sie Projektpartner werden und mit anderen Partnern kooperieren

DS: Wie ist das virtuelle Datenschutzbüro entstanden ?

MT: Die Idee zu dem Projekt hatte 1999 der Landesbeauftragte für den Datenschutz Schleswig-Holstein (jetzt: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein). Nach einem Jahr Vorlauf hatten sich die jetzigen Projektpartner zusammengefunden und die Zielsetzungen ausdiskutiert.

Die Realisierung lag und liegt hauptsächlich beim ULD SH, das auch die Server betreibt und für die nächsten 2 Jahre die Geschäftsführung des virtuellen Datenschutzbüros innehat.

Die Domain datenschutz.de gibt es schon länger als Service für alle Nutzerinnen und Nutzer, die nach Datenschutzinstitutionen suchen. Sie wurde vom Berliner Datenschutzbeauftragten betrieben, der selbst Projektpartner ist und sie freundlicherweise für das virtuelle Datenschutzbüro zur Verfügung gestellt hat.

Zukunft

Geplant ist ein weiterer Ausbau des virtuellen Datenschutzbüros, d.h. neben einer inhaltlichen Vervollständigung z.B. Einrichtung einer Projektbörse oder interessanter Expertenforen. Das virtuelle Datenschutzbüro ist unter [1] zu

erreichen. Der Berliner Datenschutzbeauftragte - vorheriger Besitzer dieser Doamin - ist nun unter www.datenschutz-berlin.de erreichbar. Übrigens ist dies ein Aufruf: Vielleicht hat ja der ein oder andere aus dem CCC ebenfalls Lust, sich als Partner an diesem Projekt zu beteiligen ? Bei Interesse meldet Euch doch bitte bei [1] (nur Koordination, wg. zeitl. Einschränkungen)

Offtopic

The Godfather, accompanied by his attorney, walks into a room to meet with his accountant. The Godfather asks the accountant, "Where's the three million bucks you embezzled from me?" The accountant doesn't answer. The Godfather asks again, "Where's the three million bucks you embezzled from me?" The attorney interrupts, "Sir, the man is a deaf-mute and cannot understand you, but I can interpret for you." The Godfather says, "Well, ask him where the @#!* money is." The attorney, using sign language, asks the accountant where the three million dollars is. The accountant signs back, "I don't know what you're talking about." The attorney interprets to the Godfather, "He doesn't know what you're talking about." The Godfather pulls out a pistol, puts it to the temple of the accountant, cocks the trigger and says, "Ask him again where the @#!* money is!" The attorney signs to the accountant, "He wants to know where it is!" The accountant signs back, "Okay! Okay! The money's hidden in a suitcase behind the shed in my backyard!" The Godfather says, "Well, what did he say?" The attorney interprets to the Godfather, "He says that you don't have the guts to pull the trigger."

[1] http://www.datenschutz.de
[1] mailto:redbaron@ccc.de

CIA MANUAL – A STUDY OF ASSASSINATION

Der "Freedom of Information Act" fördert so einiges aus den Archiven der US-Geheimdienste zutage. Unter anderem auch diese Kopie einer Anleitung der CIA für potentielle Attentäter. Der Artikel ist weniger interessant aufgrund der darin beschriebenen Techniken, sondern eher wegen der dahintersteckenden Geisteshaltung dieser Behörde.

Definition

Assassination is a term thought to be derived from "Hashish", a drug similar to marijuana, said to have been used by Hasan-Dan-Sabah to induce motivation in his followers, who were assigned to carry out political and other murders, usually at the cost of their lives. It is here used to describe the planned killing of a person who is not under the legal jurisdiction of the killer, who is not physically in the hands of the killer, who has been selected by a resistance organization for death, and who has been sele cted by a resistance organization for death, and whose death provides positive advantages to that organization.

Employment

Assassination is an extreme measure not normally used in clandestine operations. It should be assumed that it will never be ordered or authorized by any U.S. Headquarters, though the latter may in rare instances agree to its execution by membe rs of an associated foreign service. This reticence is partly due to the necessity for committing communications to paper. No assassination instructions should ever be written or recorded. Consequently, the decision to employ this technique must nearly always be reached in the field, at the area where the act will take place. Decision and instructions should be confined to an absolute minimum of persons. Ideally, only one person will be involved. No report may be made, but usually the act will be pr operly covered by normal news services, whose output is available to all concerned.

Justification

Murder is not morally justifiable. Self-defense may be argued if the victim has knowledge which may destroy the resistance organization if divulged. Assassination of persons responsible for atrocities or reprisals may be regarded as just puni shment. Killing a political leader whose burgeoning career is a clear and present danger to the cause of freedom may be held necessary.

But assassination can seldom be employed with a clear conscience. Persons who are morally squeamish should not attempt it.

Classifications

The techniques employed will vary according to whether the subject is unaware of his danger, aware but unguarded, or guarded. They will also be affected by whether or not the assassin is to be killed with the subject hereafter, assassinations in which the subject is unaware will be termed "simple"; those where the subject is aware but unguarded will be termed "chase"; those where the victim is guarded will be termed "guarded." If the assassin is to die with the subject, the act will be called "lost." If the assassin is to escape, the adjective will be

"safe." It should be noted that no compromises should exist here.

The assassin must not fall alive into enemy hands. A further type division is caused by the need to conceal the fact that the subject was actually the victim of assassination, rather than an accident or natural causes. If such concealment is desirable the operation will be called "secret" ;; if concealment is immaterial, the act will be called "open"; while if the assassination requires publicity to be effective it will be termed "terroristic." Following these definitions, the assassination of Julius Caesar was safe, simple, and terroristic, while that of Huey Long was lost, guarded and open. Obviously, successful secret assassinations are not recorded as assassination at all. [Illegible] o f Thailand and Augustus Caesar may have been the victims of safe, guarded and secret assassination. Chase assassinations usually involve clandestine agents or members of criminal organizations. THE ASSASSIN In safe assassinations, the assassin needs the usual qualities of a clandestine agent. He should be determined, courageous, intelligent, resourceful, and physically active.

If special equipment is to be used, such as firearms or drugs, it is clear that he must have outstanding skill with such equipment. Except in terroristic assassinations, it is desirable that the assassin be transient in the area. He should have an absolute minimum of contact with the rest of the organization and his instructions should be given orally by one person only. His safe evacuation after the act is absolutely essential, but here again contact should be as limited as possible. It is preferable that the person issuing instructions also conduct any withdrawal or covering action which may be necessary. In lost assassination, the assassin must be a fanatic of some sort. Politics, religion, and revenge are about the only feasible motives. Since a fanatic is unstable psychologically, he must be handled with extreme care. He must not know the iden tities of the other members of the organization, for although it is intended that he die in the act, something may go wrong. While the Assassin of Trotsky has never revealed any significant information, it was unsound to depend on this when the act was p lanned.

Planning

When the decision to assassinate has been reached, the tactics of the operation must be planned, based upon an estimate of the situation similar to that used in military operations. The preliminary estimate will reveal gaps in information and possibly indicate a need for special equipment which must be procured or constructed. When all necessary data has been collected, an effective tactical plan can be prepared. All planning must be mental; no papers should ever contain evidence of the oper ation. In resistance situations, assassination may be used as a counter-reprisal. Since this requires advertising to be effective, the resistance organization must be in a position to warn high officials publicly that their lives will be the price of rep risal action against innocent people. Such a threat is of no value unless it can be carried out, so it may be necessary to plan the assassination of various responsible officers of the oppressive regime and hold such plans in readiness to be used only i f provoked by excessive brutality. Such plans must be modified frequently to meet changes in the tactical situation.

Techniques

The essential point of assassination is the death of the subject. A human being may be killed in many ways but sureness is often overlooked by those who may be emotionally unstrung by the seriousness of this act they intend to commit. The spe cific technique employed will depend upon a large number of variables, but should be constant in one point: Death must be abso-

lutely certain. The attempt on Hitler's life failed because the conspiracy did not give this matter proper attention. Techniques may be considered as follows:

1. Manual. It is possible to kill a man with the bare hands, but very few are skillful enough to do it well. Even a highly trained Judo expert will hesitate to risk killing by hand unless he has absolutely no alternative. However, the simplest local tools a re often much the most efficient means of assassination. A hammer, axe, wrench, screw driver, fire poker, kitchen knife, lamp stand, or anything hard, heavy and handy will suffice. A length of rope or wire or a belt will do if the assassin is strong and agile. All such improvised weapons have the important advantage of availability and apparent innocence. The obviously lethal machine gun failed to kill Trotsky where an item of sporting goods succeeded. In all safe cases where the assassin may be subject to search, either before or after the act, specialized weapons should not be used. Even in the lost case, the assassin may accidentally be searched before the act and should not carry an incrimin ating device if any sort of lethal weapon can be improvised at or near the site. If the assassin normally carries weapons because of the nature of his job, it may still be desirable to improvise and implement at the scene to avoid disclosure of his identity.

2. Accidents. For secret assassination, either simple or chase, the contrived accident is the most effective technique. When successfully executed, it causes little excitement and is only casually investigated. The most efficient accident, in simple assassination, is a fall of 75 feet or more onto a hard surface. Elevator shafts, stair wells, unscreened windows and bridges will serve. Bridge falls into water are not reliable. In simple cases a private meeting with the subject may be arranged at a properly-cased location. The act may be executed by sudden, vigorous [excised] of the ankles, tipping the subject over the edge. If the assassin immediately sets up an outcry, playing the "horrified wit ness", no alibi or surreptitious withdrawal is necessary. In chase cases it will usually be necessary to stun or drug the subject before dropping him. Care is required to insure that no wound or condition not attributable to the fall is discernible after death. Falls into the sea or swiftly flowing rivers may suffice if the subject cannot swim. It will be more reliable if the assassin can arrange to attempt rescue, as he can thus be sure of the subject's death and at the same time establish a workable al ibi. If the subject's personal habits make it feasible, alcohol may be used [2 words excised] to prepare him for a contrived accident of any kind. Falls before trains or subway cars are usually effective, but require exact timing and can seldom be free from unexpected observation. Automobile accidents are a less satisfactory means of assassination.

If the subject is deliberately run down, very exact timing is necessary and investigation is likely to be thorough. If the subject's car is tampered with, reliability is very lo w. The subject may be stunned or drugged and then placed in the car, but this is only reliable when the car can be run off a high cliff or into deep water without observation. Arson can cause accidental death if the subject is drugged and left in a burning building. Reliability is not satisfactory unless the building is isolated and highly combustible.

3. Drugs. In all types of assassination except terroristic, drugs can be very effective. If the assassin is trained as a doctor or nurse and the subject is under medical care, this is an easy and rare method. An overdose of morphine administered as a sedat ive will cause death without disturbance and is difficult to detect. The size of the dose will depend upon whether the subject has been using narcotics regularly.

If not, two grains will suffice. If the subject drinks heavily, morphine or a similar narcotic can be injected at the passing out stage, and the cause of death will often be held to be acute alcoholism. Specific poisons, such as arsenic or strychine, are effective but their possession or procurement is incriminating, and accurate dosage is problematical. Poison was used unsuccessfully in the assassination of Rasputin and Kolohan, though the latte r case is more accurately described as a murder.

4. Edge Weapons Any locally obtained edge device may be successfully employed. A certain minimum of anatomical knowledge is needed for reliability. Puncture wounds of the body cavity may not be reliable unless the heart is reached. The heart is protected by the rib cage and is not always easy to locate. Abdominal wounds were once nearly always mortal, but modern medical treatment has made this no longer true. Absolute reliability is obtained by severing the spinal cord in the cervical region. This can be done with the point of a knife or a light blow of an axe or hatchet. Another reliable method is the severing of both jugular and carotid blood vessels on both sides of the windpipe. If the subject has been rendered unconscious by other wounds or drugs, either of the above methods can be used to insure death.

5. Blunt Weapons As with edge weapons, blunt weapons require some anatomical knowledge for effective use. Their main advantage is their universal availability. A hammer may be picked up almost anywhere in the world. Baseball and [illegible] bats are very widely dist ributed. Even a rock or a heavy stick will do, and nothing resembling a weapon need be procured, carried or subsequently disposed of. Blows should be directed to the temple, the area just below and behind the ear, and the lower, rear portion of the skull. Of course, if the blow is very heavy, any portion of the upper skull will do. The lower frontal portion of the head, from th e eyes to the throat, can withstand enormous blows without fatal consequences.

6. Firearms Firearms are often used in assassination, often very ineffectively. The assassin usually has insufficient technical knowledge of the limitations of weapons, and expects more range, accuracy and killing power than can be provided with reliability. Since certainty of death is the major requirement, firearms should be used which can provide destructive power at least 100% in excess of that thought to be necessary, and ranges should be half that considered practical for the weapon. Firearms have other drawbacks. Their possession is often incriminating. They may be difficult to obtain. They require a degree of experience from the user. They are [illegible]. Their [illegible] is consistently over-rated.

However, there are many cases in which firearms are probably more efficient than any other means. These cases usually involve distance between the assassin and the subject, or comparative physical weakness of the assassin, as with a woman. (a) The precision rifle. In guarded assassination, a good hunting or target rifle should always be considered as a possibility. Absolute reliability can nearly always be achieved at a distance of one hundred yards. In ideal circumstances, t he range may be extended to 250 yards. The rifle should be a well made bolt or falling block action type, handling a powerful long-range cartridge. The .300 F.A.B. Magnum is probably the best cartridge readily available. Other excellent calibers are . 375 M.[illegible]. Magnum, .270 Winchester, .30 - 106 p.s., 8 x 60 MM Magnum, 9.3 x 62 kk and others of this type.

These are preferable to ordinary military calibers, since ammunition available for them is usually of the expanding bullet type, whereas most ammunition for military rifles is full jacke-

ted and hence not sufficiently let hal. Military ammunition should not be altered by filing or drilling bullets, as this will adversely affect accuracy. The rifle may be of the "bull gun" variety, with extra heavy barrel and set triggers, but in any case should be capable of maximum precision. Ideally, the weapon should be able to group in one inch at one hundred yards, but 21/2" groups are adequa te. The sight should be telescopic, not only for accuracy, but because such a sight is much better in dim light or near darkness.

As long as the bare outline of the target is discernable, a telescope sight will work, even if the rifle and shooter are in total darkness. An expanding, hunting bullet of such calibers as described above will produce extravagant laceration and shock at short or mid-range. If a man is struck just once in the body cavity, his death is almost entirely certain. Public figures or guarded officials may be killed with great reliability and some safety if a firing point can be established prior to an official occasion. The propaganda value of this system may be very high.

(b) The machine gun. Machine guns may be used in most cases where the precision rifle is applicable. Usually, this will require the subversion of a unit of an official guard at a ceremony, though a skillful and determined team might conceivably dispose of a loyal gun crow without commotion and take over the gun at the critical time. The area fire capacity of the machine gun should not be used to search out a concealed subject. This was tried with predictable lack of success on Trotsky. The automatic feature of the machine gun should rather be used to increase reliability by placing a 5 second burst on the subject. Even with full jakket ammunition, this will be absolute lethal is the burst pattern is no larger than a man. This can be accomplished at about 150 yards. In ideal circumstances, a properly padded and targeted ma chine gun can do it at 850 yards. The major difficulty is placing the first burst exactly on the target, as most machine gunners are trained to spot their fire on target by observation of strike. This will not do in assassination as the subject will not wait.

(c) The Submachine Gun. This weapon, known as the "machine-pistol" by the Russians and Germans and "machine-carbine" by the British, is occasionally useful in assassination. Unlike the rifle and machine gun, this is a short range weapon and since it fires pistol ammu nition, much less powerful. To be reliable, it should deliver at least 5 rounds into the subject's chest, though the .45 caliber U.S. weapons have a much larger margin of killing efficiency than the 9 mm European arms. The assassination range of the sub-machine gun is point blank. While accurate single rounds can be delivered by sub-machine gunners at 50 yards or more, this is not certain enough for assassination. Under ordinary circumstances, the 5MG should be used as a fully automatic weapon. In the hands of a capabl e gunner, a high cyclic rate is a distinct advantage, as speed of execution is most desirable, particularly in the case of multiple subjects.

The sub-machine gun is especially adapted to indoor work when more than one subject is to be assassinated. An effective technique has been devised for the use of a pair of submachine gunners, by which a room containing as many as a dozen subjects can be "purifico" in about twenty seconds with little or no risk to the gunners. It is illustrated below. While the U.S. sub-machine guns fire the most lethal cartridges, the higher cyclic rate of some foreign weapons enable the gunner to cover a target quicker with acceptable pattern density. The Bergmann Model 1934 is particularly good in this way. The Danish Madman? SMG has a moderately good cyclic rate and is admirably compact and concealable. The Russian SHG's

have a good cyclic rate, but are handicapped by a small, light protective which requires more kits for equivalent killing effect.

(d) The Shotgun. A large bore shotgun is a most effective killing instrument as long as the range is kept under ten yards. It should normally be used only on single targets as it cannot sustain fire successfully. The barrel may be "sawed" off for convenience, but this is not a significant factor in its killi ng performance. Its optimum range is just out of reach of the subject. 00 buckshot is considered the best shot size for a twelve gage gun, but anything from single balls to bird shot will do if the range is right. The assassin should aim for the solar plexus as the shot pattern is small at close range and can easily [illegible] the head.

(e) The Pistol. While the handgun is quite inefficient as a weapon of assassination, it is often used, partly because it is readily available and can be concealed on the person, and partly because its limitations are not widely appreciated. While many well kn own assassinations have been carried out with pistols (Lincoln, Harding, Ghandi), such attempts fail as often as they succeed, (Truman, Roosevelt, Churchill).

If a pistol is used, it should be as powerful as possible and fired from just beyond reach. The pistol and the shotgun are used in similar tactical situations, except that the shotgun is much more lethal and the pistol is much more easily conceale d. In the hands of an expert, a powerful pistol is quite deadly, but such experts are rare and not usually available for assassination missions.

.45 Colt, .44 Special, .455 Kly, .45 A.S.[illegible] (U.S. Service) and .357 Magnum are all efficient calibers. Less powerful rounds can suffice but are less reliable. Sub-power cartridges such as the .32s and .25s should be avoided. In all cases, the subject should be hit solidly at least three times for complete reliability.

(f) Silent Firearms The sound of the explosion of the proponent in a firearm can be effectively silenced by appropriate attachments. However, the sound of the projective passing through the air cannot, since this sound is generated outside the weapon. In cases w here the velocity of the bullet greatly exceeds that of sound, the noise so generated is much louder than that of the explosion. Since all powerful rifles have muzzle velocities of over 2000 feet per second, they cannot be silenced. Pistol bullets, on the other hand, usually travel slower than sound and the sound of their flight is negligible. Therefore, pistols, submachine guns and any sort of improvised carbine or rifle which will take a low velocity cartridge can be silenc ed.

The user should not forget that the sound of the operation of a repeating action is considerable, and that the sound of bullet strike, particularly in bone is quite loud. Silent firearms are only occasionally useful to the assassin, though they have been widely publicized in this connection. Because permissible velocity is low, effective precision range is held to about 100 yards with rifle or carbine type weapons, while with pistols, silent or otherwise, are most efficient just beyond arms length. The silent feature attempts to provide a degree of safety to the assassin, but mere possession of a silent firearm is likely to create enough hazard to counter the advantage of its silence. The silent pisto l combines the disadvantages of any pistol with the added one of its obviously clandestine purpose. A telescopically sighted, closed-action carbine shooting a low velocity bullet of great weight, and built for accuracy, could be very useful to an assassin in certain situations. At the time of writing, no such weapon is known to exist.

7. Explosives. Bombs and demolition charges of various sorts have been used frequently in assassination. Such devices, in terroristic and open assassination, can provide safety and

overcome guard barriers, but it is curious that bombs have often been the imp lement of lost assassinations. The major factor which affects reliability is the use of explosives for assassination. the charge must be very large and the detonation must be controlled exactly as to time by the assassin who can observe the subject. A small or moderate explosi ve charge is highly unreliable as a cause of death, and time delay or booby-trap devices are extremely prone to kill the wrong man. In addition to the moral aspects of indiscriminate killing, the death of casual bystanders can often produce public reacti ons unfavorable to the cause for which the assassination is carried out.

Bombs or grenades should never be thrown at a subject. While this will always cause a commotion and may even result in the subject's death, it is sloppy, unreliable, and bad propaganda. The charge must be too small and the assassin is never sure of: (1) reaching his attack position, (2) placing the charge close en ough to the target and (3) firing the charge at the right time. Placing the charge surreptitiously in advance permits a charge of proper size to be employed, but requires accurate prediction of the subject's movements. Ten pounds of high explosive should normally be regarded as a minimum, and this is explosive of fragmentation material. The latter can consist of any hard, [illegible] material as long as the fragments are large enough. Metal or rock fragments should be walnut-size rather than pen-size. If solid plates are used, to be ruptured by the explosion, cast iron, 1" thick, gives excellent fragmentation. Military or commercial high explosives are practical for use in assassination.

Homemade or improvised e xplosives should be avoided. While possibly powerful, they tend to be dangerous and unreliable. Anti-personnel explosive missiles are excellent, provided the assassin has sufficient technical knowledge to fuse them properly. 81 or 82 mm mortar shells, or the 120 mm mortar shell, are particularly good. Anti-personnel shells for 85, 88, 90, 100 and 105 mm guns and howitzers are both large enough to be completely reliable and small enough to be carried by one man. The charge should be so placed that the subject is not ever six feet from it at the moment of detonation. A large, shaped charge with the [illegible] filled with iron fragments (such as 1" nuts and bolts) will fire a highly lethal shotgun-type [illegible] to 50 yards. This reaction has not been thoroughly tested, however, and an exact replica of the proposed device should be fired in advance to determine exact range, pattern-size, and penetration of fragments.

Fragments should penetrate at lea st 1" of seasoned pine or equivalent for minimum reliability. Any firing device may be used which permits exact control by the assassin. An ordinary commercial or military explorer is efficient, as long as it is rigged for instantaneous action with no time fuse in the system. The wise [illegible] electric target can serve as the triggering device and provide exact timing from as far away as the assassin can reliably hit the target. This will avid the disadvantages olitary or commercial high explosives are practical for use in assassination. Homemade or improvised explosives should be avoided. While possibly powerful, they tend to be dangerous and unreliable. Anti-personnel explosive missiles are excellent, provided the assassin has sufficient technical knowledge to fuse them properly. 81 or 82 mm mortar shells, or the 120 mm mortar shell, are particularly good. Anti-personnel shells for 85, 88, 90, 100 and 105 mm guns and howitzers are both large enough to be completely reliable and small enough to be carried by one man. The charge should be so placed that the subject is not ever six feet from it at the moment of detonation. A large, shaped charge with the [illegible] filled with iron fragments (such as 1"

nuts and bolts) will fire a highly lethal shotgun-type [illegible] to 50 yards.

This reaction has not been thoroughly tested, however, and an exact replica of the proposed device should be fired in advance to determine exact range, pattern-size, and penetration of fragments. Fragments should penetrate at least 1" of seasoned pine or equivalent for minimum reliability. Any firing device may be used which permits exact control by the assassin. An ordinary commercial or military explorer is efficient, as long as it is rigged for instantaneous action with no time fuse in the system. The wise [illegible] electric target can serve as the triggering device and provide exact timing from as far away as the assassin can reliably hit the target. This will avid the disadvantages of stringing wire between the proposed positions of the ass assin and the subject, and also permit the assassin to fire the charge from a variety of possible positions. The radio switch can be [illegible] to fire [illegible], though its reliability is somewhat lower and its procurement may not be easy. EXAMPLES ([illegible] may be presented brief outlines, with critical evaluations of the following assassinations and attempts: Marat Hedrich Lincoln Hitler Harding Roosevelt Grand Duke Sergei Truman Pirhivie Mussolini Archduke Francis Ferdinand Benes Rasputin Aung Sang Madero [illegible] Kirov Abdullah Huey Long Ghandi Alexander of Yugoslvia Trotsky http://www.bobharris.com/cooldocs/ciamanual.html.

Join the "stop police abuse" list at [1] People Against Racist Terror (PART), PO Box 1055, Culver City, CA 90232 Tel.: 310-495-0299 E-mail: [2] < URL : [3] Send for a sample of our quarterly print publication: "Turning The Tide: Journal of Anti-Racist Action, Research & Education"

---

*[1] http://*www.egroups.com/group/stop-polabuse
*[2] mailto:*part2001@usa.net
*[3] http://*www.antiracist.org/issues.html

Machtstrukturen und Zensur im Internet

von Dragan Espenschied und Alvar Freude

Im Rahmen unserer Diplom-Arbeit, deren Thema Machstrukturen im Internet ist, haben wir an unserer Hochschule ein recht aufwändiges Experiment zum Thema Zensur und Manipulation von Internet-Sites durchgeführt. An Kommentaren und Anregungen wären wir sehr interessiert.

Kurz zum Hintergrund der Hochschule: Die Merz Akademie bildet Kommunikations-Designer aus. Im Gegensatz zum reinen Grafikdesign wird an der Akademie besonderen Wert auf kulturtheoretische Zusammenhänge und kritischem Umgang mit Medien gelegt. Theorie und Forschung nehmen über die Hälfte der Vorlesungen ein. Seit dreieinhalb Jahren ist das Gebäude komplett vernetzt, jeder Rechner bietet Zugang zum Internet. Das Angebot wird stark genutzt; Kurse zum Thema sind überbelegt.

Unser Experiment befasst sich mit der hierarchischen Struktur des Internets und der dadurch möglichen Manipulation von Inhalten: Wir setzten einen selbstentwickelten Proxy-Server auf und stellten ganz simpel an jedem uns zugänglichen Rechner diesen Proxy für HTTP-Zugriffe in den Browsern ein. Nun fließt also der gesamte (nur unverschlüsselte) Web-Traffic durch diesen Proxy, der darauf ausgelegt ist, die Anfragen nicht nur in einer Datenbank anonym zu protokollieren, sondern auch die zurückkommenden HTML-Seiten vor dem Weiterreichen an den anfragenden Browser zu manipulieren. Die Surfer bemerken dabei nichts, alle URLs bleiben erhalten, jedoch kann von einzelnen Worten bis zu kompletten Sites alles verändert oder vollständig ausgetauscht und neue Domains eingeführt werden. Niemand außer unserer Dozentin (Prof. Olia Lialina) wusste von dem Projekt.

Natürlich legen wir Wert darauf, keine personenbezogenen Daten etc zu speichern. Mit dem Experiment wollen wir herausfinden mit welchem Aufwand eine solche zentrale Zensursoftware verbunden ist, welche Reaktionen die Manipulationen hervorrufen, wie unsere unfreiwilligen Versuchspersonen mit dem Web umgehen und welches Bild sie vom Medium im allgemeinen haben.

Vorausgreifend: Die durchgeführten Manipulationen halten wir für verhältnismäßig brisant. Die Reaktionen der "Testpersonen" auf die Manipulationen und erst recht der Bekanntgabe derselben in einer Mail an alle mit dem Betreff "Internet-Manipulation an der Merz-Akademie – Hintergründe und wie man es abschalten kann", blieben zu unserer Überraschung nahezu vollkommen aus. Für uns drängt sich der Eindruck auf, dass Desinteresse und Hilflosigkeit vorherrschen.

u.a. die folgenden Manipulationen nehmen wir vor:

• Die Namen von Gerhard Schröder und Helmut Kohl werden vertauscht. Dies geschieht auch, wenn nur der Familienname genannt wird. Laut allen Nachrichten- und Magazin-Sites veröffentlicht nun also Gerhard Schröder sein Tagebuch und Gerhard Schröder wurde in Spendenaffären verwickelt. – Das hört sich vielleicht ein wenig simpel an, jedoch funktioniert

die Sinnverdrehung in den allermeisten Fällen perfekt. Selbst wenn unter einem Foto, auf dem Kohl ein wenig angeschlagen guckt, steht, Gerhard Schröder würde ein Tagebuch veröffentlichen, gibt es wieder eine passende Bedeutung. http://online-demonstration.org/insert_coin/proxy-bilder/kohl-tagebuch.gif

• Der Name von Al Gore wurde gegen Al Bundy ausgetauscht.

• Die Worte "und", "oder" und "aber" wurden mit einer gewissen Wahrscheinlichkeit ausgetauscht. Dieser simple Trick kann den Inhalt eines Textes komplett verdrehen.

In den vier an der Akademie beliebtesten Freemail-Diensten (GMX, hotmail, mail.com und Yahoo!) fügten wir die frei erfundene "Global Penpals Association" ein: In einem nicht übersehbaren großen Kasten, von Farbigkeit und Layout an die entsprechenden Services angepasst, wird ein "Brieffreund" mit Foto und kurzer Beschreibung vorgestellt. Über einen Button kann dieser Person sofort eine Nachricht aus dem Freemailer geschickt werden. Im Kasten steht außerdem der Hinweis, dass diese Person "für Sie aufgrund Ihrer persönlichen Einstellungen und Ihres Surfverhaltens" ausgesucht wurde. Wir haben acht Personen bei verschiedenen Freemail-Diensten erfunden, die zufällig angezeigt werden und sich recht schnell wiederholen. Wir stellten außerdem eine einfache Feedback-Möglichkeit durch ein Formular bereit, angeblich an die Initiatoren der Global Penpals Association.

Weiterhin haben wir die sieben meistbenutzten Suchmaschinen so verändert, dass jede dort gefundene Seite ein Formular von "netzgegenrechts.yahoo.de" enthält, in dem man die Möglichkeit hat, die gefundene Seite anonym als pornografisch, rassistisch, gotteslästerlich, kinderpornografisch, geschäftsschädigent, urheberrechtsverletzend oder anstößig beim Suchmaschinen-Betreiber zu melden. Auch hier gab es die Möglichkeit des Feedbacks über ein Formular oder Email-Adresse. Wir haben auch gruselige Erklärungstexte verfasst, in denen unter anderem von "Kein Schmutz im Internet!" und "Zivilcourage" die Rede ist. [1] Außerdem werden 2% aller Webzugriffe auf eine Werbeanzeige umgeleitet. Diese kommt angeblich von InterAd.gov, einer fiktiven Vereinigung von ICANN, Corenic, Internic und des Amerikanischen Wirtschaftsministeriums. Die Begründung lautet: Da die US-Regierung sämtliche Core-Server betreibt, müssten diese irgendwie finanziert werden. Jede Anzeige fordert die Surfer außerdem dazu auf, einzugeben, wie viele US-Dollars sie für ein bestimmtes Produkt monatlich ausgeben würden. Welches Produkt das ist richtet sich nach der Anzeige, beworben werden die US-Marines, die National Rifle Association, Novartis, Garth Brooks, eine Burger-Kette etc. Erst wenn hier ein Wert eingegeben wurde, kommen die Surfer wirklich auf die Seite, die sie eigentlich erwartet haben. Darauf wird auch im Anleitungstext deutlich hingewiesen. Ohne diese Eingabe bleibt der Browser auf der Anzeigen-Seite hängen, selbst der Back-Button funktioniert nicht mehr. Auch hier war Feedback möglich.

Napster konnten wir verändern, da der Windows-Client zum Start des Programms über einen eingebetteten Internet-Explorer eine Seite von napster.com darstellt. Von dort aus öffneten wir ein rahmenloses Fenster über den gesamten Bildschirm, in dem man von Bertelsmann aufgefordert wird, unsinnig persönliche Daten zur Teilname am Napster preiszugeben.

Als letztes bekamen die Studenten auf ihren eigenen Homepages und Projekt-Homepages Popup-Anzeigen von der Merz Akademie untergejubelt: "Click here for good education!"

---

[1] http://online-demonstration.org:8888/netzgegenrechts.yahoo.de/

Einige oft besuchte Seiten bekamen zudem kleine Veränderungen oder komplette Umleitungen verpasst. Beliebte Flash-Animationen werden gegen eine immer gleiche, unglaublich häßliche Animation gewechselt. Wir tauschen viele weitere Worte, beispielsweise wird Nahost zu Balkan und Bombe zu Torte etc.

All diese Manipulationen waren nur innerhalb der Merz Akademie aktiv. An der Akademie gibt es ungefähr 240 Studenten, wovon jeden Tag bis zu circa 150 erscheinen. Wie viele das Web nutzen wissen wir nicht genau. Durch unseren Proxy gingen täglich 100 bis 300 MB Daten, Spitzentage brachten bis zu 2 GB. Aufgerufen werden vor allem Freemailer, Suchmaschinen, eigene Webprojekte, Design-Sites, Kataloge und – natürlich – Warez-Sites.

Die Reaktionen verliefen ganz anders als erwartet. Zuerst waren wir sehr vorsichtig und setzen die Manipulationen noch vereinzelt oder mit einer geringen Wahrscheinlichkeit ein. Wir merkten jedoch bald, dass wir alle Register bis zum Anschlag ziehen konnten, ohne dass irgend jemand Verdacht schöpfen würde. Die Napster-Manipulation wurde schnell umgangen, da das Fenster einfach mit einem Tastaturbefehl zu schließen ist. Der Austausch der Politikernamen blieb bis auf einen Fall unbemerkt: ein Student druckte sich eine besonders gelungene Seite bei Spiegel-Online aus.

Auch bei der Global Penpals Association stellte fast niemand die Frage, woher diese denn eventuell über das Surfverhalten oder die persönlichen Einstellungen Bescheid wissen könne, wo doch jeder Freemail-Service beteuert, letztere Daten nicht herauszugeben. Nur ein Student schrieb eine entsprechende Nachricht. Und das war auch noch der selbe, dem der Austausch von Schröder und Kohl aufgefallen war.

Die Suchmaschinenveränderung von netzgegenrechts.yahoo.de wurde kritiklos hingenommen. Es ist nicht einmal ein stiller Protest durch den Wechsel zu anderen Suchmaschinen erkennbar. Es wurde nicht ein einziges Mal die Informationsseite zu dieser Aktion aufgerufen.

Die Popups auf den eigenen Homepages wurden ebenso hingenommen, reflexartiges Schließen des Werbefensters konnten wir jedoch mehrmals beobachten. Unseren Testpersonen scheint also nicht klar zu sein, woher normalerweise solch ein Werbefenster kommt. Dass jemand scheinbar an ihren Daten herumändert scheint nicht weiter wichtig.

Das InterAd-Programm hingegen könnte man beinahe als Erfolg bezeichnen. Ein Student beschwerte sich bei der erfundenen InterAd-Behörde und schaute sich sogar die Informationsseite an. Weitere beschwerten sich, scheinbar ohne den zwei Sätze umfassenden und deutlichst sichtbaren Erklärungstext gelesen zu haben, bei der technischen Assistenz der Hochschule. Nur eine verschwindend geringe Anzahl von Studenten gaben Werte bei der Frage, wie viele Dollars sie monatlich für Feuerwaffen usw. ausgeben würden, ein. Immerhin kamen sie dadurch weiter auf die Seite, die sie eigentlich sehen wollten. Alle anderen schlossen einfach das Browser-Fenster.

Aufgeflogen ist unsere zwei Wochen dauernde Manipulation nur, weil durch einen Speicher-Defekt unser gesamter Server ausfiel und dadurch ungefähr einen halben Tag keine Web-Zugriffe mehr möglich waren. Die technische Assistenz merkte, dass die Rechner betroffen waren, an denen unser Server als Proxy eingestellt war.

Daraufhin klärte unsere Dozentin die Technische Assistenz und die Verwaltung über das Projekt auf. Einen Tag später schickte der Werkstattleiter eine Mail an alle Dozenten und Studenten, in der er darauf hinwies, dass wir Kreditkartennummern mitprotokolliert haben könnten. Das führte zu keiner Reaktion. Erst

am nächsten Tag schickten wir eine Nachricht an alle, in der wir genau erklärten, dass wir den gesamten Web-Traffic manipulieren (die Details zu einzelnen Filtern führten wir nur unvollständig aus) und wie unser Projekt funktioniert, welchen Zweck es verfolgt. Wir lieferten einen Link auf eine von uns aufgesetzte Anleitungsseite, welche beschreibt, wie der Proxy auszuschalten ist.

Das ist nun vier Tage her [1], Reaktionen gab es bisher keine nennenswerten. Ein Student kam auf uns zu und fragte, ob wir seine Homepage nun manipuliert hätten, er wolle sich damit schließlich bewerben. Die Seite mit der Anleitung wurde 6 mal abgerufen, und das auch noch von Rechnern aus, die nicht durch unseren Proxy gingen. Fakt ist, dass der Proxy einfach auf den meisten Rechnern weiterläuft – wenn sich die technische Assistenz nicht darum gekümmert hat. Interessant ist auch, dass wir nicht für die Manipulationen beschuldigt wurden, sondern für das angebliche Sammeln von Kreditkartennummern, was man mit jedem Firewall oder Packet-Sniffer machen könnte. Sind die Inhalte im Web denn egal? Selbst wenn ein Großteil der Studenten das Web zur Recherche und für Freemailer nutzt?

Der Aufwand für unsere Software hielt sich in Grenzen. Wir sind nur zu zweit und haben innerhalb von vier Monaten ein recht komfortables und leistungsfähiges Programm geplant und umgesetzt. Die Manipulationsmöglichkeiten sind umfangreich, nur wenige weitere Features wären "wünschenswert". Den Traffic an der Akademie zu überwachen stellt durch ein weiteres Datenbank-Tool, mit dem wir verschiedene URLs in Kategorien einteilen können, für zwei Personen trotz der verhältnismäßig großen Diversität der abgerufenen Sites kein Problem dar. Größere Netzwerke zu manipulieren ist also durchaus möglich.

[1] Anm. d. Red.: Die mail von Dragan und Alvar erreichte uns am 12.12.2000 – also kurz nach Redaktionsschluss der ds73. Der Proxy ist aber nachwie vor erreichbar, ebenso die Homepage des Experiments http://online-demonstration.org/insert_coin/

Vorläufiges Fazit

Wir gingen zu Beginn des Experiments davon aus, dass aufgrund der eingangs erwähnten medienkritischen Ausbildung das Projekt anders aufgenommen würde als beispielsweise vom typischen AOL-User. Dennoch wurden selbst obskure Manipulationen hingenommen, besonders hervorstechend der Suchmaschinen-Blockwart-Service. Die Möglichkeiten zur direkten Beschwerde oder auch nur Kontaktaufnahme wurden nicht genutzt. Die Leute scheinen nicht das Gefühl zu haben, irgendetwas erreichen zu können, sondern sehen sich in der Konsumentenrolle.

Nach dem öffentlichen Vorwurf des Leiters unserer Medienwerkstatt, wir würden persönliche Daten ausspähen, passierte nichts weiter. Vier Erlärungsmöglichkeiten: Entweder die Leute vermuten, dass diese Behauptung falsch ist, sie verstehen nicht, was das zu bedeuten hatte, es ist ihnen egal oder sie lesen ihre Mails nicht. Auf die darauf folgende Richtigstellung von uns, wir hätten "nur" die Inhalte manipuliert, geschah ebensowenig. Auch hier ist es den Leuten entweder egal, sie haben es nicht verstanden, oder auch diese Nachricht einfach nicht gelesen. Uns würde interessieren, was Ihr dazu denkt, ob ihr zu ähnlichen Schlussfolgerungen kommen würdet und welche Beobachtungen Ihr zu diesem Thema bereits eventuell gemacht habt.

Als nächstes werden wir weitere Betroffene befragen, ob und wie sie die Manipulationen oder zumindest die Nachricht darüber aufgenommen haben. Wenn jemand den Proxy selbst ausprobieren möchte, er läßt sich auch von außen einstellen: Proxy für http: 195.226.105.73 bzw. student.merz-akademie.de Port: 7007

Webapplikationen mit JavaServer Pages

von Hans Bergsten

Überall ist die Rede von dynamischen Webseiten und Webapplikationen. JavaServer Pages sind eine gute Möglichkeit für hoch komplexe Aufgaben.

Am Anfang war das Web eine riesige Enzyklopädie, eine fast unendliche Sammlung miteinander verlinkter Texte. Dann kamen Bilder, Töne und auch kleine Animationen und Filme. Das Web wurde bunt, aber es war weiterhin statisch - die Seiten und Bilder sind nichts weiter als Dateien, die in einem Server-Verzeichnis abgelegt sind. Und trotz "Multimedia" ist dieses blosse Einweg-Kommunikation: Der Server sendet, der Client empfängt.

Dabei gibt es viele Gründe, den statischen Rahmen zu verlassen und Webseiten dynamisch zu generieren: Informationen können ständig aktualisiert werden, auf Benutzer(-gruppen) oder bestimmte Endgeräte zugeschnitten werden. Bestimmte Geschäftsanwendungen, Kommunikations- und Transaktionsmodelle, erfordern situativ angepasste Seiten. Komplexe Webseiten mit wiederkehrenden Elementen können in einzelne Teile zerlegt werden, die dann leichter zu pflegen sind und aus unterschiedlichen Quellen kommen, aber als ganze Seite an den Benutzer geschickt werden. Teilinformationen kommen aus unterschiedlichen Quellen, usw.

Der Webentwickler benötigt für solche Anwendungen einen Rahmen, d.h. Sprache und Werkzeuge, mit denen er diese entwickeln und programmieren kann.

Eine gute Webapplikation trennt die statischen Elemente von den dynamischen, sie ist weitgehend modular. Damit kann ein umfangreiches Projekt in mehrere Schritte aufgeteilt werden: Designer, Redakteure und Programmierer können ihre Bereiche entwickeln und pflegen, und über JavaServer Pages als Rahmen ihre Arbeiten integrieren. Z.B. kann der Java-Progammierer die Prozesslogik programmieren und dem Designer als Komponente zu Verfügung stellen, dieser schreibt sie als JSP-Tags direkt in den HTML-Code. Wenn später die Programmierung geändert wird, bleiben die Schnittstellen erhalten.

HTML-Forms und CGI-Skripte sind der erste Ansatz für eine Interaktion. Auf der Webseite macht der Benutzer Eingaben in einem HTML-Formular, die dann an den Server geschickt (Request) und dort von einem CGI-Skript verarbeitet werden. Das CGI-Skript stellt anhand der Eingabewerte und sonstiger Variablen die Antwort zusammen, übergibt diese an den Server, der sie dann an den Client sendet (Response).

Cookies sind eine Möglichkeit, den Benutzer über mehrere Seitenaufrufe hinweg wiederzuerkennen (Session-Management). Wenngleich Cookies durch das Anlegen und Ausspähens von Benutzerprofilen in Verruf gekommen sind.

Ein weiterer Ansatz für eine server-seitige Dynamik sind Server Side Includes. Das sind bestimmte Tags innerhalb einer Webseite, sozusagen Platzhalter, an deren Stelle der Server beim Seitenaufruf bestimmte Inhalte einsetzt. PHP folgt demselben Prinzip, geht aber mit den Möglichkeiten über SSI hinaus.

Client-seitige Techniken, Java Script und Applets, scheiden meistens aus, da ausserhalb des eigenen (Unternehmens-)Netzes sehr verscheidene Clients zu bedienen sind, die alle den jeweiligen Code unterschiedlich interpretieren.

Für server-seitige Webapplikationen gibt es zwei Konzepte:

1. Die Anfrage wird an ein Modul geleitet (http://www/servlets/some?a=x&b=y). Das Modul entscheidet anhand der Anfrageparameter, auf welche Resource(n) es zugreifen soll und wie es diese als Antwort an den Client zurückschickt:

```
out.println("<HTML>");
out.println("<BODY>");
out.println("<P>Heute ist" + new
java.util.Date());
out.println("...");
out.println("</HTML>");
```

Beispiele für das Modul-orientierte Konzept sind Java Servlets, CGI-Skripte.

2. Die Anfrage richtet sich an eine Datei (http://www/other.jsp?a=x&b=y), die ihrerseits von einem Modul gelesen wird, das dann die in der Seite zwischen den HTML-Tags eingebetteten Befehle ausführt:

```
<HTML> <BODY> <P>Heute ist <%= new
java.util.Date() %> ... </HTML>
```

Zu dieser Gruppe gehören JavaServer Pages, Server Side Includes, PHP und andere.

In beiden Fällen greift ein Modul auf eine Resource zu (Datei, Datenbankeintrag usw.), führt bestimmte Befehle aus und generiert daraus die Antwort. Genaugenommen funktionieren auch statische Webseiten so: Ein Modul (bei Apache ist das der default-handler) liest eine Datei und reicht diese an die Ausgabe weiter.

Das erste Konzept betont die Prozesslogik, das Modul erzeugt den HTML-Code. Beim zweiten Konzept liegt der Schwerpunkt auf der einzelnen Seite - das HTML-Gerüst liegt vor und integriert die dynamischen Elemente.

Weil Server Pages von dem HTML-Seitenparadigma ausgehen, sind sie einfacher zu erlernen. Das ist auch der Grund für die grosse Verbreitung von PHP und anderen. Dabei sind sie eine Untergruppe des ersten Konzepts. Server Pages werden oft auch als inside-out-Module bezeichnet.

Der Vorteil von JavaServer Pages [1] gegenüber anderen Server Pages liegt in der Flexibilität und dem Umfang der Möglichkeiten, die Java mitbringt. Die Funktionen von JavaServer Pages können mittels weiterer Klassen, Java Beans und Tag Libraries, erweitert werden.

Java selbst ist durchgehend objektorientiert und eignet sich gut, vergleichsweise einfach sehr komplexe Webapplikationen zu entwikkeln. Ausserdem können Java Servlets und JavaServer Pages auf die gesamten Java APIs zurückgreifen: JDBC, JRMI, EJB usw. (Hinzu kommen die immer wieder genannten Vorteile von Java: Platformunabhängigkeit, Skalierbarkeit usw.)

Die Flexibilität und der Umfang von Java ist gleichzeitig auch ihr grösster Nachteil. Ohne eine Java Virtual Machine geht nichts. Aktuelle Versionen von Servlet- und JSP-Containern verlangen nach der neuesten Java-Version, diese ist dann nicht immer für alle Betriebssysteme verfügbar. Und auch die objektorientierte Sprache verlangt einige Aufmerksamkeit, damit nicht am Ende riesige Klassenbibliotheken wegen einer einfachen Funktion geladen werden müssen.

Die Vorteile von Java zahlen sich erst ab einer gewissen Grösse bzw. Komplexität aus - kleinere Webapplikationen sind leichter in Perl oder PHP entwickelt als mit Java. Eine funktio-

[1] http://java.sun.com/products/jsp/

nierende JSP-Umgebung vorausgesetzt, bieten JavaServer Pages allerdings einen leichten Einstieg und man wird schnell die Möglichkeiten dieser Sprache zu schätzen lernen.

Eine solche Servlet- und JSP-Umgebung ist Apache Tomcat [1]. Diese funktioniert als Webserver, ist OpenSource und gleichzeitig die Referenzimplementation für Java Servlets und JavaServer Pages. Wer bereits ein Java Development Kit installiert hat, hat auch den Apache-Tomcat-Server schnell eingerichtet. Dieser kommt mit Beispielen für Java Servlets und JavaServer Pages - auf Suns JSP-Webseite [1] finden sich Tutorials und die Spezifikationen.

Zum Buch

Zu JavaServer Pages erschien vor wenigen Wochen ein Buch bei O'Reilly [2]. Wie viele Bücher aus dem O'Reilly-Verlag ist auch dieses ein guter Leitfaden zu dieser Technologie, sowohl als Einführung als auch als Nachschlagewerk. Das Buch ist gut strukturiert und sehr ausführlich. Die vielen Beispiele lassen einen das dargestellte unmittelbar praktisch nachvollziehen.

Dieses Buch richtet sich an (Java-)Programmierer und HTML-Schreiber. Wer sich mit Webapplikationen und JavaServer Pages beschäftigen möchte (jeder Hacker sollte das, Anm. von Tom) und das nötige Kleingeld übrig hat, für den ist dieses Buch eine gute Investition. Die deutsche Übersetzung erscheint voraussichtlich im August. **<arne>**

Hans Bergsten, JavaServer Pages, Verlag O'Reilly, ISBN: 1-56592-746-X *USD 39.95*

[1] http://jakarta.apache.org/
[2] http://www.oreilly.de/catalog/jserverpages/

Hackers At Large 2001: debating the future of the Internet.

August 9th until August 12th 2001, University of Twente, Netherlands

From August 9th until August 12th, the campus of the University of Twente will feature a congress that is unique in its kind: Hackers at Large, or HAL 2001. The congress expects to receive thousands of guests from all over the world and from many different disciplines to debate issues ranging from advanced technical issues regarding some obscure aspect of the Internet to easy-to-understand lectures on some of the dangers of the information society, as well as many, many other topics. But more than debate, the guests at HAL2001 take ample time to get on-line, relax, build and discuss cool stuff, and engage in good old analog interfacing.

The congress is unique in that the participants bring their tent and their computer, which is connected to a large high-speed outdoor computer network that provides high bandwidth Internet connectivity for everybody. On-site power generators provide all these computers with the necessary power: more than 1.5 mega-Watts.

Some of the people that are organizing HAL 2001 were also involved in the former hacker movement in The Netherlands: those responsible for the late hackers' magazine Hack-Tic and for setting up the first Internet Service Provider in The Netherlands called ``XS4ALL''. But also many people from Dutch universities, companies and other Internet Service Providers participate in making this event possible.

The HAL2001 convention is the fourth in a series that has been running every four years since 1989. Quite a few of the participants at "The Galactic Hacker Party" (1989), "Hacking at the End of the Universe" (1993) and "Hacking in Progress" (1997) have been instrumental in bringing about the changes that are upon us today.

HAL2001 is for those that can truly celebrate the Internet and embrace new technologies, without forgetting their responsability to tell others that all these wonderful new technologies come with new risks to the individual and to society as a whole.

(Quelle: Pressemitteilung)

Easter(H)egg 2001

13.4.2001 - 16.4.2001, *Eidelstedter Bürgerhaus, Hamburg*

Dieses Jahr über Ostern (13.04.2001 bis 16.04.2001) findet das erste Easter(H)egg statt. Im Gegensatz zum Congress in Berlin oder den Veranstaltungen des Chaos-Bildungswerks in Hamburg soll das Easter(H)egg keine Vortragsveranstaltung sein, sondern Anfassen und Mitdenken ist das Motto: In zahlreichen ganztägigen Workshops werden Themen zur Computersicherheit, Netztechnik, Amateurfunk und Gesellschaft ausführlich behandelt, diskutiert und gleich praktisch umgesetzt. Dabei tragen alle Teilnehmer der Workshops durch aktive Mitarbeit zum Gelingen bei. Aus diesem Grund wird es auch kein Hackcenter geben. Wegen des familiären Charakters der Veranstaltung ist die Zahl der Teilnehmer begrenzt. Eine vorherige Anmeldung ist daher zwingend erforderlich. Weitere Informationen und genaues Programm unter

*http://*www.hamburg.ccc.de/eh2001

Bestellungen, Mitgliedsanträge und Adressänderungen bitte senden an:

CCC e.V., Lokstedter Weg 72, D-20251 Hamburg

Adressänderungen und Rückfragen auch per E-Mail an: office@ccc.de

- Satzung + Mitgliedsantrag
  DM 5,00
- Datenschleuder-Abonnement, 8 Ausgaben
  Normalpreis DM 60,00 für
  Ermässigter Preis DM 30,00
  Gewerblicher Preis DM 100,00 (Wir schicken eine Rechnung)
- Alte Ausgaben der Datenschleuder auf Anfrage
- Chaos CD blue, alles zwischen 1982 und 1999
  DM 45,00 + DM 5,00 Portopauschale

Die Kohle

- liegt als Verrechnungsscheck bei
- wurde überwiesen am ___.___.____ an
  Chaos Computer Club e.V., Konto 59 90 90-201
  Postbank Hamburg, BLZ 200 100 20

Name: _____

Strasse: _____

PLZ, Ort: _____

Tel., Fax: _____

E-Mail: _____

Ort, Datum: _____

Unterschrift: _____

Süddt Ztg

Dienstag, 20. Februar 2001

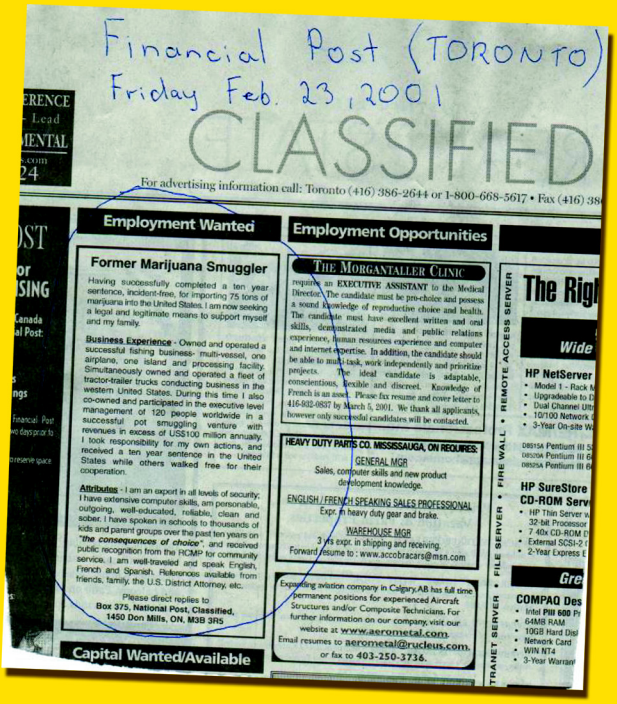
COMPUTER UND INTERNET

Fidel der Hacker

Admiral sieht Kubas Computer als Gefahr

Fidel Castro, Kubas alternder Revolutionsheld, ist der größte Hacker aller Zeiten. Das glaubt zumindest der amerikanische Admiral Tom Wilson, Leiter des militärischen Geheimdienstes *Defense Intelligence Agency*. Einem Komitee des US-Senats sagte Wilson, der *Maximo Lider* bereite womöglich eine Computerattacke auf die USA vor. „Sie haben einen starken Geheimdienst, gute Sicherheitstechnik und das Potenzial, unser Militär durch asymmetrische Taktik durcheinander zu bringen." Und damit meinte der Admiral: „Informations-Kriegsführung oder Angriffe auf Computer-Netzwerke, um damit unseren Zugang zu der Region oder die Verlegung von Truppen zu stören". Der CIA-Direktor George Tenet warnte in der selben Sitzung, dass der Terrorist Osama bin Laden moderne Verschlüsselungs-Software benutze, um die Kommunikation seiner Organisation vor Geheimdiensten zu schützen. Beobachter in Washington erwarten, dass der US-Kongress nach diesen Warnungen die Export-Richtlinien für Verschlüsselungsprogramme verschärfen könnte. *cris*

Tarnen und Täuschen war einst das Motto von Spionen. Die Tarnung übt Fidel Castro offenbar schon. Reuters


Financial Post (TORONTO)
Friday Feb. 23, 2001

CLASSIFIED

For advertising information call: Toronto (416) 386-2644 or 1-800-668-5617 • Fax (416) 38

Employment Wanted

Former Marijuana Smuggler

Having successfully completed a ten year sentence, incident-free, for importing 75 tons of marijuana into the United States. I am now seeking a legal and legitimate means to support myself and my family.

Business Experience - Owned and operated a successful fishing business- multi-vessel, one airplane, one island and processing facility. Simultaneously owned and operated a fleet of tractor-trailer trucks conducting business in the western United States. During this time I also co-owned and participated in the executive level management of 120 people worldwide in a successful pot smuggling venture with revenues in excess of US$100 million annually. I took responsibility for my own actions, and received a ten year sentence in the United States while others walked free for their cooperation.

Attributes - I am an export in all levels of security. I have extensive computer skills, am personable, outgoing, well-educated, reliable, clean and sober. I have spoken in schools to thousands of kids and parent groups over the past ten years on "*the consequences of choice*", and received public recognition from the RCMP for community service. I am well-traveled and speak English, French and Spanish. References available from friends, family, the U.S. District Attorney, etc.

Please direct replies to
Box 375, National Post, Classified,
1450 Don Mills, ON, M3B 3R5

Capital Wanted/Available

Employment Opportunities

THE MORGANTALLER CLINIC

requires an **EXECUTIVE ASSISTANT** to the Medical Director. The candidate must be pro-choice and possess a sound knowledge of reproductive choice and health. The candidate must have excellent written and oral skills, demonstrated media and public relations experience, human resources experience and computer and internet expertise. In addition, the candidate should be able to multi-task, work independently and prioritize projects. The ideal candidate is adaptable, conscientious, flexible and discreet. Knowledge of French is an asset. Please fax resume and cover letter to 416-932-0837 by March 5, 2001. We thank all applicants, however only successful candidates will be contacted.

HEAVY DUTY PARTS CO. MISSISSAUGA, ON REQUIRES:

GENERAL MGR
Sales, computer skills and new product development knowledge.

ENGLISH / FRENCH SPEAKING SALES PROFESSIONAL
Exp. in heavy duty gear and brake.

WAREHOUSE MGR
3 yrs expr. in shipping and receiving.
Forward resume to : www.accobracars@msn.com

Expanding aviation company in Calgary,AB has full time permanent positions for experienced Aircraft Structures and/or Composite Technicians. For further information on our company, visit our website at www.aerometal.com
Email resumes to aerometal@rucleus.com, or fax to 403-250-3736.

The Righ
Wide
HP NetServer
HP SureStore
CD-ROM Serv
COMPAQ Des