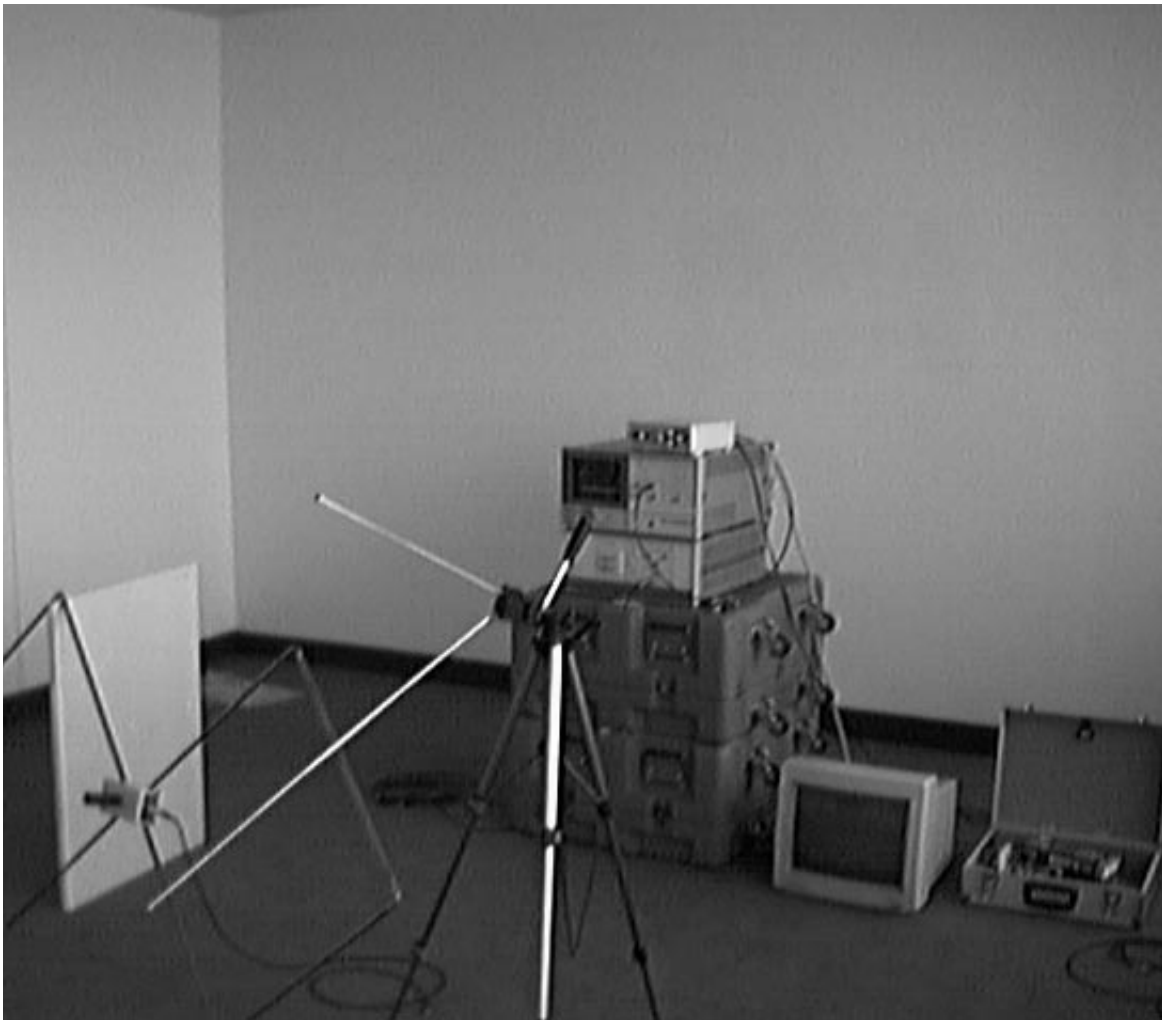
Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club



- *Anwerbeversuch des BND in der Hackerszene*
- *Paradigmenwechsel und Ignorantentum*
- *Gehacktes: Premiere, GSM, SSL...*

ISSN 0930-1045
Sommer 1998, DM 5,00
Postvertriebsstück C11301F

#63

Impressum

Die Datenschleuder Nr. 63
II. Quartal, Sommer 1998

Herausgeber:
(Abos, Adressen etc.)
Chaos Computer Club e.V.,
Schwenckestr. 85, D-20255 Hamburg,
Tel. +49 (40) 401801-0,
Fax +49 (40) 4917689,
EMail: office@ccc.de
Redaktion:
(Artikel, Leserbriefe etc.)
Redaktion Datenschleuder,
Postfach 642 860, D-10048 Berlin,
Tel +49 (30) 285 986 00
Fax +49 (30) 285 986 56
EMail: ds@ccc.de
Druck: St. Pauli Druckerei Hamburg
ViSdP: Wau Holland
Mitarbeiter dieser Ausgabe:
Andreas Bogk (andreas@ccc.de), Andy Müller-Maguhn (andy@ccc.de), Frank Rieger (frank@ccc.de), Tron (tron@ccc.de), Christine (musidora@zedat.fu-berlin.de), Pluto (pluto@pizzaservice.de), Tobias (tobias@ccc.de), Wau Holland (wau@ccc.de)
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.

Adressen

Chaos im Internet: http://www.ccc.de & news:de.org.ccc

Erfa-Kreise des CCC

Hamburg: Treff jeden Dienstag, 20 Uhr in den Clubräumen in der Schwenckestr. 85 oder im griechischen Restaurant gegenüber. U-Bahn Osterstraße / Tel. (040) 401801-0, Fax (040) 4917689, EMail: ccc@hamburg.ccc.de

Berlin: Club Discordia Donnerstags alle zwei Wochen 17-23 Uhr in den Clubräumen, Marienstraße 11, Hinterhof, Berlin-Mitte, Nähe Bahnhof Friedrichstraße, Tel. (030) 28598600, Fax (030) 28598656, EMail: ccc@berlin.ccc.de. Briefpost: CCC Berlin, Postfach 642860, D-10048 Berlin.

Chaosradio auf Fritz i.d.R. am letzten Mittwoch im Monat von 22.00-01.00 Uhr, Aufzeichnungen der Sendungen im Internet abrufbar, Feedback an chaos@orb.de, http://chaosradio.ccc.de.

Bielefeld: CCC Bielefeld: Treff jeden Dienstag um 20 Uhr in der Gaststätte Extra, Siekerstraße 23, Bielefeld. Kontakt: M. Gerdes (0521) 121429, EMail: ccc@bielefeld.ccc.de.

Köln: Chaos Computer Club Cologne (C4), Bobstr. 28, (Ecke Clemensstraße), 50676 Köln. Treff jeden Dienstag um 19:30 in den Clubräumen (Chaoslabor), Telefonischer Kontakt via 0177-2605262.

Mönchengladbach: Treff: Dienstags um 19:30 im Surfer's Paradise, Bahner 19 in Mönchengladbach. Kontakt via gregor@ccc.de

Die Liste der CCC-Treffs der anderen Städte findet ihr aktuell immer auf http://www.ccc.de/ChaosTreffs.html

Chaos Family

Bielefeld: FoeBuD e.V., Treff jeden Dienstag um 21.00 Uhr im Café (Wissens)Durst in der Heeper Str. 64. PUBLIC DOMAIN Veranstaltungsreihe: jeden 1. Sonntag im Monat ab 15 Uhr im Bunker Ulmenwall, Kreuzstr. 0. siehe http://www.foebud.org/. Briefpost: FoeBuD e.V., Marktstr. 18, D-33602 Bielefeld, Fax. (0521) 61172, Mailbox (0521) 68000, Telefon-Hotline (0521) 175254, Mo-Fr 17-19 Uhr. EMail: foebud@bionic.zerberus.de. http://www.foebud.org.

Stuttgart: Computerrunde Suecrates, norman@delos.stgt.sub.org.

Österreich: Public Netbase, http://www.t0.or.at/
Engagierte ComputerexpertInnen, Postfach 168, A-1015 Wien ?

USA: 2600, http://www.2600.com

Editorial

- ❑ **Liebe(r) LeserInnen,**
- ❑ **Sehr geehrte Damen und Herren,**
- ❑ **Werte Freaks,**
- ❑ ✳❃❋❄❉▲▲✲◆●●❄■
- ❑ **Herr Außenminister Kinkel,**
- ❑ **Herr Schmidtbauer,**
- ❑ **Werte Abgeordnete,**
- ❑ **Liebe Netzgemeinde**
- ❑ **Chaoten**
- ❑ **Diskordier**
- ❑ **besorgte Mütter**
- ❑ **gutmütige Väter**
- ❑ **Sicherheitsbeauftragte**
- ❑ **Wasauchimmer**

Zum Geleit gibt es diesmal schon aus Zeitgründen nicht viel zu sagen. Eigentlich wollten wir euch ja schon vor 2 Wochen mit dieser Datenschleuder bewerfen - die Liste der Gründe, warum das nicht geklappt hat ersparen wir uns.

Wichtig: wir wollen mehr Autoren. Wir wollen Informationen, Daten, Wissenswertes, Konspiratives, halböffentliches, Details, Namen, Daten und Zeugen.

Für jeden Artikel, der es bis in die Datenschleuder schafft, gibt es 1 Jahr frei die Datenschleuder (4 Ausgaben oder mehr).

Anonyme Zusendungen explizit erwünscht. Nachprüfbares Material bzw. Quellenangaben oder Verweise hilfreich (von wegen der journalistischen Sorgfaltsdingsda).

Schicken an:

ds@ccc.de oder die

Red. Datenschleuder,

Postfach 640236, D-10048 Berlin

Habt einen schönen Sommer.

AMM

Index

BND versucht Hacker anzuwerben

Aktivitäten des Bundesnachrichtendienstes (BND) in der Hackerszene

In einer Zeit, in der Geheimdienste zwar evolutionär längst als überholt erscheinen, faktisch jedoch noch nicht abgeschafft sind, passieren seltsame Dinge. Die folgende Geschichte passierte weder an fremdem Ort, noch in ferner Zeit.

Der Junge Hacker Ulrich Unbedarft* studiert ein bisschen vor sich hin, arbeitet nebenbei in einer Art Computerfirma und hat die wilden Zeiten des Hackens eigentlich schon längst hinter sich gelassen. Er ist zwar erst Anfang Zwanzig, hat aber als junger Mensch genug Ältere erlebt, deren Hochmut und Größenwahn Ihnen einen Haufen Probleme gebracht hat. Insofern kann man ihn als braven Staatsbürger betrachten: er verdient legal sein Geld, geht regelmässig zur Uni, versteuert sein Einkommen und hält sogar bei Rot an der Ampel. Und wenn da nicht dieses klitzekleine Problem mit der Wehrmacht wäre, die sich vorgenommen hatte, seine Menschenrechte anzugreifen, indem sie ihm zum Waffentaug-lichkeitstest zwingen wollte, dann wäre er sogar da gemeldet, wo er wohnt.

Eines Tages bekommt er an seiner Arbeitsstelle einen Anruf. Da meldet sich ein gewisser Paul Geldgier* und stellt sich als freier Mitarbeiter einer „Unternehmensberatung“ vor. Er hätte da ein Problem, wo Ulrich Unbedarft ihm vielleicht helfen könne und etwas Geld verdienen könnte. Die Unternehmensberatung würde für unterschiedliche Kunden ihre Dienste anbieten. Ein Investor, der in einem fremden Land in Computertechnologie investieren wollte, würde gerne sichergehen, auch nichts Falsches zu machen. Daher wäre es für ihn wichtig zu erfahren, welche Form von Technologie dort schon eingesetzt würde. Es ginge letztlich um Netzwerkprodukte - Details müssten als Geschäftsgeheimnisse geschützt bleiben - und die Frage wäre ganz konkret, welche Form von Computernetzwerken in diesem Land schon vorhanden wären. Ulrich Unbedarft - ob man ihm schon an dieser Stelle Naivität vorwerfen kann, sei dahingestellt - hatte keine Bedenken. Ein Treffen wurde vereinbart, um die Details des Auftrages zu besprechen.

Zum Treffen reiste Geldgier offenbar von fernen Gefilden an. Man verabredete sich in irgendeinem Cafe, später auch mal in einem Hotel - Geldgier war stets pünktlich und zuverlässig. Geldgier hatte - damit Unbedarft auch ja nichts vergessen würde - schriftliche Fragenkataloge mitgebracht. Ulrich Unbedarft fand das alles normal, checkte die IP-Nummern und die dort registrierten Computer und andere technische Parameter dort ab (nichts Verbotenes) und lieferte prompt. Geldgier drückte ihm 2000.- DM in bar in die Hand und ließ sich eine Quittung unterschreiben. Ulrich war erstmal glücklich - man fühlt sich ja nicht jeden Tag angemessen bezahlt...

So weit, so gut. Dann ging das irgendwie ein paar Wochen so weiter. Ein anderes Land kam in das Visier des „Investors“ und damit auch - mit Fragenkatalog - auf Ulrichs Schreibtisch. Diesmal war die Region ein bisschen eingegrenzt. Und dann waren da noch ein paar zusätzliche Fragen zum Internet im Zielland. Technisch kein Problem, legal, prompt bezahlt. So schön einfach kann das Leben sein, dachte sich Ulrich.

Eines Tages wollte Paul Geldgier noch ein bißchen mehr. Geldgier berichtete von der Zufriedenheit mit der Arbeit von Ulrich und daß er da jemanden getroffen hätte. Dieser jemand - schon etwas konspirativ, ohne Namen - hätte die Arbeitsergebnisse von Ulrich ebenfalls gesehen und hätte das sehr interessant gefunden. Dann hätte sich der Namenlose als Mitarbeiter des Bundesnachrichtendienstes (BND) ausgewiesen

Der „kritische Dialog“ in der Praxis

[redacted] Consulting GmbH

[redacted]

Tel.: 0[redacted] / [redacted]
Fax: 0[redacted] / [redacted]

- Welche Internetprovider bieten neben IPM ihre Dienste im IRN an? ✓
- Welche Rolle spielt das Postministerium in Teheran?
- Hängen IPM (als physikalischer Knoten) und das Postministerium (als Provider) zusammen?

Früher hatte das IPM über zwei Standleitungen über die UNI Wien Zugriff auf das Internet. Dies ist offensichtlich nicht mehr der Fall!

- Seit wann und warum wurde der Zugang geändert?
- Welche Bandbreite steht über die Kabelverbindung zum italienischen Provider zur Verfügung?
- Wer betreibt die iranische Bodenstation für den Satellitenzugang zum kuwaitischen Provider?

- Wie erhalten Unternehmen Zugang zum Internet?
- Gibt es einen zentralen Zugangsknoten?

- Welche Erkenntnisse gibt es zu Zensurmaßnahmen durch iranische Stellen?
- Wie werden evtl. Zensurmaßnahmen in der Praxis umgesetzt?
- Welche Regelungen gibt es zur Verschlüsselung, bzw. den Einsatz von Steganographie?

Geschäftsführer:
[redacted]

Amtsgericht Oldenburg, HRB-Nr. 3012

Bankverbindung:
Deutsche Bank [redacted]
[redacted]
Postbank [redacted]
[redacted]

Bundesnachrichtendienstdilletanten oder:

und folgendes Anliegen vorgebracht: ob er denn nicht mal richtig hacken könnte. Also, es ginge da um Informationen aus Computern des bereits erforschten Ziellandes über Forschungsprojekte bei A(tomaren), B(iologischen) und C(hemischen) Waffen. Ein Staatsanwalt würde das ganze vorher absegnen, um die Legalität sicherzustellen. Und einen Haufen Geld könnte er sich dabei auch verdienen.

Da hatte Ulrich Unbedarft dann erst einmal ein Adrenalinproblem und bat sich etwas Bedenkzeit aus. Paul Geldgier hatte auf einmal einen ganzen Koffer voll Argumente dabei. Er könne sein Land vor großem Schaden schützen, sogar wertvolle Dienste für sein Vaterland leisten. Diese Anliegen waren in Ulrich Wertesystem allerdings nicht hinreichend verankert. Und irgendwie waren ihm Waffen und Geheimdienste auch nie symphatisch gewesen.

So bekam Ulrich dann das, was man nicht nur beim Chaos Computer Club als kalte Füße bezeichnet. Aber immerhin, waren die Füße dann noch intakt genug, um ihn zu uns zu tragen. So konnten wir im halböffentlichen Konspirations-sofa sitzen und überlegen, was zu tun sei. Denn so ganz eindeutig und klar war die Geschichte ja nicht. Ist Paul Geldgier wirklich mit einem vom BND zusammengetroffen? Oder gibt es den Mann vom BND gar nicht? Ist Paul´s Auftraggeber vielleicht ein ganz anderes Land und Ulrich vielleicht schon längst - unwissentlich - in geheimdienstlichen Agententätigkeit verstrickt? Beim BND anrufen erschien zwecklos; die würden das ja nicht bestätigen, sondern eher nach dem NSA-Motto („never say anything“) agieren.

Am Telefon konnte man die Sache schon mal gar nicht besprechen. Wir entschieden uns einen - als integer angesehenen und mit offiziellen Kontakten versehenen Anwalt als Vermittler einzuschalten. Der mußte erstmal überlegen und machte einen Vorschlag zum schnellen vorgehen. Denn das Problem war sozusagen die tickende Uhr. Unbedarft hatte sich gegenüber Geldgier eine Frist von einigen Tagen auserbeten um sich das mit dem Projekt zu überlegen. Dann sollte es ein neues Treffen geben. Das könnte aber - nachdem Ulrich jetzt klargeworden war, daß er da in eine Sache verstrickt wurde mit der er gar nichts (im Sinne von: Null) zu tun haben wollte - auch gefährlich sein. Vielleicht würde ihn Paul erpressen? Vielleicht kommt auf einmal ein Sturmtrupp von der Wehrmacht vorbei? Vielleicht wird der aggresiv oder droht mit Rache für den Fall einer Veröffentlichung?

Der überlegte Schlachtplan lautete wie folgt: Anwalt ruft beim BND an; und zwar bei einer so hinreichend hohen Stelle, daß eine gegenseitige Deckung niederer Mitarbeiter ausgeschlossen werden kann. Wobei der Anwalt gleich sagt: erstmal schalten die den Radarschirm an und überwachen alle, die ihm Verdacht stehen damit zu tun zu haben. Und egal was ist, werden Sie nicht sagen „wir warn´s“ oder „wie warn´s net“. „Wir können das weder bestätigen noch dementieren.“ ist die Standartantwort. Die Entwicklung interaktiver Kommunikation hat gesellschaftlich noch längst nicht alle Kreise erfaßt...

Es sollte dem BND unmißverständlich mitgeteilt werden, dass Ulrich keinen Kontakt mit derartigen Kreisen wünscht. Und dann zieht Geldgier sich entweder zurück oder die Spionageabwehr ruft bei Ulrich an und krallt sich Geldgier beim nächsten Treffen. Denkt man da so, in seiner naiven Art.

Aber irgendwie kam alles ganz anders. Schon einen Tag später, zurück in der heimischen Stadt mit den vielen Baustellen klingelte das Telefon bei Unbedarft. Geldgier erkundigte sich, was denn passiert sei. Er wäre da nach Pullach für den morgigen Tag zitiert und wüsste gar nicht, warum. Ob Unbedarft was wüsste?

Informationen preisgeben durch Fragen stellen

[redacted] Consulting GmbH

[redacted]

Tel.: [redacted]
Fax: [redacted]

Region St. Petersburg, hier insb. Universitäten (u.a. die Baltic State Technical University)

Fragen bzgl. dort vorhandener Netzwerken:

- Welche Hard- und Software wird bei den Clients eingesetzt?
- Welche Serversoftware wird eingesetzt; welche Art von Server wird eingesetzt?
- Welche Übertragungsprotokolle kommen zum Einsatz?
- Welche Verkabelung bzw. Netzwerkkarten kommen beim Netz zum Einsatz?
- Wie läuft die Verteilung der Adressen im Netz ab (DHCP????)?
- In welchem Umfang werden Informationen übertragen?
- Welche Art von Informationen werden übertragen (Dateien oder Mail)?
- Welche und wieviele Nutzer sind mit dem Netz verbunden bzw. welche Institutionen sind an das Netz angeschlossen?
- Welche Verbindungen zu anderen Datennetzen existieren innerhalb des Netzes?

Geschäftsführer:
[redacted]

Amtsgericht Oldenburg, HRB-Nr. 3012

Bankverbindung:
Deutsche Bank [redacted]
[redacted]
Postbank [redacted]
[redacted]

Unbedarft ist vielleicht naiv, aber blöd auch wieder nicht und sagt deswegen: nein. Und Geldgier sagt, er meldet sich dann morgen nochmal, nach dem Termin in Bayern. Und so ging der Alptraum erstmal weiter.

Und anstatt sich endlich dahin zu verziehen, wo er hingehört (liegt auch in Bayern), nervte Geldgier am nächsten Tag nach seinem Termin in Pullach schon wieder. Da seien ja offensichtlich einige Mißverständnisse abgelaufen und er möchte ja nicht, daß sich das niederschlägt - nicht daß es da noch Auswirkungen auf seine Auftragslage gibt und er keine Aufträge mehr bekäme. Geldgier hatte offenbar schlechte Laune und Angst, Geld zu verlieren. Und bettelte und bat um ein Treffen. Irgendwie hatte Unbedarft auch Mitleid mit Geldgier, von ansatzweisem Verständnis zu sprechen wäre zuviel. Also gut, ein letztes Treffen in einem Cafe in Berlin, dachte er sich - lieber Ende mit Schrecken als Schrecken ohne Ende.

Ulrichs Zielsetzung zum Treffen war ihm klar: unmißverständlich die Sache zu Ende führen. Was allerdings Geldgier von ihm wollte, war ja nicht so ganz klar. Und so schien es sinnvoll, für den Fall minder harmonischer Gesprächsstimmungen und Andeutungen jemanden mitzunehmen. Ein offizieller Vertreter des CCC mußte also mit. In der Rolle hatte ich natürlich nicht nur die Intention, diese Anfrage abzulehnen, sondern diesen Kreisen unmißverständlich mitzuteilen: eine Anwerbung von Hackern durch Nachrichtendienste wird von uns in aller Entscheidenheit abgelehnt und darf nicht wieder vorkommen. Wir haben mehr als ein Todesopfer durch Geheimdienstverstrickungen in der Hackerszene zu verzeichnen; ob das dann im Kino rüberkommt, ist eine andere Frage.

Aber die Gelegenheit, dies diplomatisch am Cafetisch zu klären, ergab sich nicht - ein Grund mehr, daß ganze hier und andernorts zu veröffentlichen. Geldgier erschien nicht. Auf Ulrichs Mobilbox fand sich auf einmal eine Nachricht von Geldgier: „er säße in einem Taxi vor´m <Treffpunkt> und ihm wäre was dazwischengekommen“. Ein Foto, einen Kaffee sowie ein Eis später war klar, daß sich zumindest niemand offen zeigen würde.

Ich halte es nicht für notwendig, jetzt noch moralische Zeigefinger zu erheben oder viele Zeilen zu schreiben. Die Fragebögen sprechen für sich. Ulrich will eigentlich nur seine Ruhe haben; die können wir ihm allerdings angesichts der Brisanz der Geschichte im Bezug auf den Lernwert für die Hackerszene nur bedingt versprechen. Und noch einmal: auf Geheimdienste haben wir keinen Bock. Wir machen öffentliche Arbyte, keine geheime. Das Problem an Geheimdiensten ist ja nicht nur die auch in der Wirtschaft übliche NDA-Vorgehensweise (non disclosure agreement), sondern auch die Verstrickungen und Erpressungen, die als Begleiterscheinungen für eine „Kontinuität“ des Arbeitsverhältnisses sorgen. Geheimdienste wollen im Kern das Gegenteil von dem, was Hacker wollen: Wissen geheimhalten, um Prozesse zu verlangsamen und für bestimmte Leute steuerbar machen. Hackern wollen offenen Umgang und Steuerbarkeit für diejenigen, die es betrifft.

Auch an andere: Selbstregulierende kalte Füße sind sicherlich hilfreicher als externe Kaltmachung. Gegen Erpressung durch persönliche Geheimnisse hilft Offenheit. Think future compatible.

Andy Müller-Maguhn, andy@ccc.de

Neues aus der freien Marktwirtschaft

Microsoft conducts nuclear test

REDMOND (BNN)—World leaders reacted with stunned silence as Microsoft Corp. (MSFT) conducted an underground nuclear test at a secret facility in eastern Washington state. The device, exploded at 9:22 am PDT (1622 GMT/12:22 pm EDT) today, was timed to coincide with talks between Microsoft and the US Department of Justice over possible antitrust action.

„Microsoft is going to defend its right to market its products by any and all necessary means," said Microsoft CEO Bill Gates. „Not that I'm anti-government" he continued, „but there would be few tears shed in the computer industry if Washington were engulfed in a bath of nuclear fire."

Scientists pegged the explosion at around 100 kilotons. „I nearly dropped my latte when I saw the seismometer" explained University of Washington geophysicist Dr. Whoops Blammover, „At first I thought it was Mt. Rainier, and I was thinking, damn, there goes the mountain bike vacation."

In Washington, President Clinton announced the US Government would boycott all Microsoft products indefinitely. Minutes later, the President reversed his decision. „We've tried sanctions since lunchtime, and they don't work," said the President. Instead, the administration will initiate a policy of „constructive engagement" with Microsoft.

Microsoft's Chief Technology Officer Nathan Myrhvold said the test justified Microsoft's recent acquisition of the Hanford Nuclear Reservation from the US Government. Not only did Microsoft acquire „kilograms of weapons grade plutonium" in the deal, said Myrhvold, „but we've finally found a place to dump those millions of unsold copies of Microsoft Bob." Myrhvold warned users not to replace Microsoft NT products with rival operating systems. „I can neither confirm nor deny the existence of a radioisotope thermoelectric generator inside of every Pentium II microprocessor," said Myrhvold, „but anyone who installs an OS written by a bunch of long-hairs on the Internet is going to get what they deserve."

The existence of an RTG in each Pentium II microprocessor would explain why the microprocessors, made by the Intel Corporation, run so hot. The Intel chips „put out more heat than they draw in electrical power" said Prof. E. Thymes of MIT. „This should finally dispell those stories about cold fusion."

Rumors suggest a second weapons development project is underway in California, headed by Microsoft rival Sun Microsystems. „They're doing all of the development work in Java," said one source close to the project. The development of a delivery system is said to be holding up progress. „Write once, bomb anywhere is still a dream at the moment."

Meanwhile, in Cupertino, California, Apple interim-CEO Steve Jobs was rumored to be in discussion with Oracle CEO Larry Ellison about deploying Apple's Newton technology against Microsoft. „Newton was the biggest bomb the Valley has developed in years," said one hardware engineer. „I'd hate to be around when they drop that product a second time."

Paradigmenwechsel

Zwei Themen/Thesen:

a) Was wir bisher an rechtlichem Trouble gegen das Netz gesehen haben, ist nur der Vorbote dessen, was wir bekommen, sobald Connectivity billiger und durchlaufende Server Commodities werden.

b) Das bisher beobachtete Jugendschutz-Paradigma wird spätestens dann scheitern.

Längere Version:

Bisher ist es so, daß der durchschnittliche Haushalt daheim keinen durchlaufenden Rechner hat, der die anderen Maschinen eines Haushalts (und dazu gehören auch WinCE-Devices wie Waschmaschinen, Fernseher, Videorecorder, WebTVs und Spielconsolen) mit Daten versorgt. Bisher ist es auch so, daß der durchschnittliche Haushalt keine dauerhafte bidirektionale Verbindung zu externen Netzen hat.

Dadurch bekommen wir etwas, das dem Paradigma des „Point“ in Tiernetzen sehr ähnlich ist, mit dem Provider als „Sysop“ aka Erbringer von Mehrwertdiensten und dem Kunden als „Point“, der von seinem Sysop gescheucht, kontrolliert und beaufsichtigt werden soll.

Werden eigene Leitungen in Haushalte häufiger und wandern Mehrwertdienste erst einmal vom Provider in die Haushalte ab, wird sich diese Situation verändern: Sobald Haushalte eigene Mail-, Web- und Proxyserver haben, wird der Provider für einen guten Teil dieser Haushalte vom Erbringer von Mehrwertdiensten wieder zum reinen Päckchenschubser degradiert (andere Haushalte werden statt eines Internet- einen Intranet-Anschluß haben, der auf die Proxy-Dienste des Providers angewiesen ist, um mit dem Internet zu kommunizieren - siehe Metronet). Inhalte werden nicht mehr auf Servern eines Providers publiziert, sondern auf dem eigenen lokalen Server - außerhalb des Haushalts existieren nur noch Cache-Copies. Artikel und Mails werden nicht mehr über einen Server eines Providers publiziert, sondern auf dem lokalen Server - der Provider leitet nur noch weiter.

In einem solchen Szenario fällt die Providerverantwortung, wie sie in den existierenden Gesetzen skizziert wird, auf die Extremfälle zusammen. Die Kontrollfunktion, die die aktuelle Rechtslage versucht, den Providern aufzudrücken, wird durch die Provider nicht mehr wahrnehmbar, sobald die Kunden sich ihre Dienste selbst erbringen (und immer mehr Kunden tun das - wer Webseiten entwickelt, hat auch einen Personal Web Server am laufen und könnte, die Leitung vorausgesetzt, dort auch publizieren).

Gesellschaftlich existiert praktisch keine Kontrolle darüber, ob ein Haushalt einen durchlaufenden Server hat oder nicht und ob auf diesem Server Publikationsdienste erbracht werden. Nach Martin Rost :-) ist das auch irrelevant, da die weltverändernde Funktion durch den Prozeß des Publizierens erbracht wird. Das bedeutet, daß das gesellschaftliche Regulativ für die oben beschriebene Situation nicht die Server beim Endanwender sind, sondern die Leitungen zum Endanwender. Sobald die Kommunikationskosten für Festverbindungen klein genug werden und die zur Verfügung stehenden Leitungskapazitäten groß genug, wird sich die Situation in der von mir beschriebenen Weise verändern.

Preislich liegt der Punkt in der Nähe dessen (Faktor 2), was ein Netsurf-Zugang jetzt kostet, d.h. sobald Datenfestverbindungen in die Region

von 70 DM rutschen (zum Vergleich: GEZ mtl. 28.50 DM, plus Kabelfernsehgebühr ~30 DM mtl. -> etwa dieselbe Summe; die Telekom-Rechnung der meisten Haushalte liegt ebenfalls in diesem Bereich).

Was ich hier die ganze Zeit versuche zu erklären, ist die Tatsache, daß Kommunikation in Datennetzen letztendlich nur zuverlässig zu fassen ist, wenn man sich ausschließlich auf die Endpunkte der Kommunikation konzentriert. In ihrer Direktheit und der Vielfalt der Kommunikationsmethoden und Dienstübergänge entzieht sich der ganze Rest dazwischen einer faßbaren Systematik und auch in gewisser Weise einer zuverlässigen rechtlichen Greifbarkeit - so er denn überhaupt existiert.

Und das ist genau das NEUARTIGE am Internet, die Qualität die es von jedem anderen Kommunikationsmedium unterscheidet, das jemals zuvor existiert hat: Zwar haben wir ein Massenkommunikationsmittel, aber alle einzelnen Kommunikationen sind Individualkommunikationen, die in zunehmendem Maße auch personalisiert werden (Man denke nur an die ganzen My-Irgendwas-Services und den Portalhype, der zur Zeit hip ist) und die mit einer Publishing Pipeline der Länge Null abgewickelt werden (Mittlerfreie Kommunikation).

Keiner der rechtlichen Rahmen, die derzeit in Deutschland gestrickt werden oder wurden, werden dieser neuartigen Qualität gerecht: Die bestehenden rechtlichen Ideen sind entweder aus dem Bereich der Rundfunkgesetzgebung oder aus dem Bereich der Telekommunikationsgesetze abgeleitet. Die Rundfunkgesetzgebung berücksichtigt aber nicht den personalisierten Charakter der Kommunikation, während die Telekommunikationsgesetze nicht die entstehende Öffentlichkeit berücksichtigen. Und die Mittlerfreiheit findet in keinem von beiden ausreichenden Niederschlag, weil öffentliche Kommunikation bisher niemals mittlerfrei war.

Gerade der Jugendschutz, der hier so heiß diskutiert wurde, hat so seine Probleme mit der Mittlerfreiheit. Es ist ja gerade das Wesen des Jugendschutzes, so wie er bisher in Deutschland gelebt wurde, daß er sich an den Mittlern einer Kommunikation orientiert hat und versucht hat, die vermittelten Inhalte zu kontrollieren oder zu beschränken. Bei Kommunikationsformen, die sich direkt zwischen Autor und Leser abspielen, greift solche Art der Kontrolle überhaupt nicht.

Was hier gebraucht wird, ist aber keine Veränderung des Netzes (die ist auch überhaupt nicht möglich: Die Entstehung von etwas wie dem Internet ist eine zwangsläufige Folge der Verbilligung von Kommunikation und der enormen Zunahme der Teilnehmerzahlen sowie des Zusammenwachsens von Informations- undKommunikationstechnologien), sondern ENDLICH eine Veränderung der Paradigmen bei denjenigen Leuten, die damit umgehen.

Und genau das Fehlen dieses Verstehens ist der Grund dafür, warum ich mich hier und andernorts immer so aufrege.

Kristian Koehntopp <kris@koehntopp.de>
debate@fitug.de

Der Nagra Hack

...oder warum jetzt plötzlich alle Premiere gucken können

Ende Mai geschah, was Kenner der Szene schon lange erwartet hatten. Die Zeit für den Premiere Hack war gekommen. Nicht daß es da nicht schon vorher Ansätze gegeben hätte. So kursierten einige Schaltpläne für einen Syster/Nagra Decoder im Internet (Syster oder Nagravision heisst das Verschlüsselungsverfahren mit dem auch untern anderem Premiere verschlüsselt ist). Premiere war sicherlich schon ein wenig beunruhigt, als die ersten Nachbauten auf den Markt kamen, basierte doch ein Teil der Sicherheit auf der Tatsache, daß die Decoder (fast) außschließlich vermietet wurden und somit an den Besitz des bezahlten Keys gebunden waren.

Aber nun ist ein kleines Programm hinzugekommen, daß es mit Hilfe eines high-end PC und fast jeder PC Fernseh Karte, die auf dem BT848 Chip basiert, ermöglicht, Premiere in nahezu perfekter Qualität zu gucken. Erstaunlich dabei ist, daß dies sogar in Farbe funktioniert. Premiere zu hacken galt Jahrelang als DIE Herrausforderung auf dem Gebiet der Videoverschlüsselung (Ein Gerücht lautet sogar, Premiere hätte 10.000,00 DM gewettet, daß es nicht geht).

Es wird wohl 1993 oder so gewesen sein, als Markus Kuhn eine interessante Idee formulierte, wie wohl die mit videocrypt verschlüsselten, brittischen Sky Kanäle dem Publikum auf dem Festland zugänglich gemacht werden könnten (die einfachste und preisgünstigste Methode ist wohl, einen Britten zu kennen, der einem die original Karte schickt). Bei Videocrypt wird jede Zeile an einer beliebigen Stelle zerhackt und die beiden Hälften werden vertauscht. Der Decoder tauscht die Zeilen gemäß der gut verschlüsselten Informationen in der Austastlücke wieder zurück. Die Decoder-Hardware kann hierbei schön billig sein, da nur RAM für jeweil eine einzige Zeile nötig ist und sich auch der Restaufwand in Grenzen hält. Der Angriff funktioniert genialerweise auf rein statistischer Basis, ohne Kentnis interner Geheimnisse. Zwei aufeinanderfolgende Videozeilen, so die Überlegung, sollten einander normalerweise sehr ähnlich sein. Schiebt man jetzt eine Zeile solange in eine Richtung (wobei man das, was hinten über ist, vorne wieder anhängt) bis sie der vorherigen am ähnlichsten ist (tolle FFT Anwendung) und macht man das für alle Zeilen, so hat man schon mal das Bild rekonstruiert, nur daß es noch irgendwie aus zwei Hälften besteht, die mitteinander vertauscht sind. Diese Stelle kann man finden und somit auch das original Bild wieder herstellen. Schade nur, man braucht ne Cray oder so, um damit realtime TV zu gucken. Das Programm heißt antisky, die sourcen finden sich...., na wo wohl.

Bei Syster/Nagravision werden die Positionen der Zeilen permutiert. Der Decoder hat RAM für 32 Zeilen und da schreibt er auch erstmal die letzten 32 Zeilen eines verschlüsselten Halbbildes rein bevor irgendwas anderes passiert. Das sind nämlich die ersten 32 Zeilen des decodierten Halbbildes, was man auch sehr schön erkennt, wenn man sich das verschlüsselte Bild mal anschaut. Danach schiebt er Zeile für Zeile an den Fernseher und holt sich für jede Zeile die er rausschiebt sofort eine neue. Die Reihenfolge bestimmt, wie bei videocrypt, ein pseudo random number generator, der durch einen verschlüsselten seed gestartet wird. Der Prozessor und die gesammte restliche Hardware wird duch den Zeilentakt des Videosignals getaktet, damit eine hundertprozentige Synchronizität gewährleistet werden kann.

Schon 1994 gab es ein Programm von einem Spanier (es gibt auch etliche spanische, französische, türkische usw. Programme, die

TV/Videocrypt Faleraklimbimpingpong

syster/nagra verschlüsselt sind), daß die gemittelten Grauwerte von jeweils zwei Zeilen addiert. Das tut es für alle möglichen Zeilenpaare. Die Paare mit den kleinsten Summen liegen direkt untereinander (meistens). Damit lässt sich die korrekte Reihenfolge wieder herstellen. Das Programm heißt antinagra. Es dauerte aber nun noch 4 Jahre, bis das Performanceproblem zumindest für syster/nagra gelöst wurde. Ein pfiffiger Franzose war es wohl, der genug über den pseudo random number generator des Decoders herausfand, um festzustellen, daß dieser genau 32768 (256x128) verschiedene Permutationen erzeugen kann und wie er das macht. Er schrieb ein Programm, daß sich ein paar wenige Zeilen des verschlüsselten Bildes nach der antinagra Methode anschaut und dann prüft, welche der 32768 Permutationen am besten dazu passt. Die Permutation, die am besten korrelliert, wird auf das ganze Bild angewandt. Es reicht, sich etwa 12 Zeilen anzuschauen und von diesen auch nur jeweils 16 Punkte. Das schafft ein P133 immerhin schon 18 mal pro Sekunde, mit einigen Verbesserungen des Algorithmus, um schneller auf die Permutation schliessen zu können, als alle auszuprobieren, sogar 25 mal. Was fehlte, war, zumindest bei einem PAL Videosignal, die Farbe. Die geht nämlich verloren, da bei PAL zum Decodieren des Farbsignales zwei aufeinanderfolgende Zeilen benötigt werden (Phase Alternate Line). Da die Farbdecodierung aber in der Framegrabber Hardware passiert und zu diesem Zeitpunkt die Zeilen des verschlüsselten Bildes nicht aufeinanderfolgen, muß das schiefgehen.

„Naja“, könnte man sagen, „decodieren wir die Farbe halt in Software“. Leider dauert das viiiieeeel zu lange. Daß es trotzdem geht, haben wir zum einen dem Umstand zu verdanken, daß bei PAL ein Burst die Phasenlage des Farbsignals der Zeile bestimmt, welcher bei der Verschlüsselung nicht permutiert wird. Normalerweise wird bei zwei aufeinanderfolgenden Zeilen die Phase durch den Burst um jeweils 180 Grad gedreht, was ja gerade zu der Farbsignalverbesserung führen soll. Zum anderen kann man glücklicherweise beim BT848 diese Farbkorrektur abschalten, so daß man die rohe Farbinformation erhält. Diese liegt in YUV vor und muß nun noch in RGB umgerechnet werden, nachdem die Zeilen in die richtige Reihenfolge gebracht wurden.

Auf einem PII 266 geht nagra decodieren und Farbe umrechnen 25 mal pro sekunde, so daß man damit schon vernünftig Premiere gucken kann. Was uns allerdings am meisten freut, bei allzu homogenen Bildern, also zuviel Fußballfeld oder zuviel nackter Haut, greift der Korrellationsalgorithmus nicht :-). Aber was macht das schon, Fernsehhacken ist sowieso spannender als Fersehgucken.

```
Weitere Infos gibts unter
http://www.ccc.de/tvcrypt
```

Und bitte löchert mich nicht mit Fragen, wo Ihr das Programm herbekommt oder daß bei euch dies oder das nicht geht. Wir werden ohnehin die Software, die nicht im Source verfügbar ist nicht weiter unterstützen. Die Linuxversion heißt NagraTV und findet sich unter wechselnder URL irgendwo auf http://www.eurosat.com. An einer Diskussion um das Verfahren und die Theorie sind wir natürlich immer interessiert.

steini@ccc.de

Telekommunikationskundenschutz-

§ 16 Abs. 1: Beschreibt das, was schon immer passierte, wenn eine überhöhte Rechnung reklamiert wurde. Es wird - auch ohne vorherigen Auftrag des Kunden - ein Einzelverbindungsnachweis für den fraglichen Zeitraum erstellt und eine „technische Prüfung“ durchgeführt, also eine Zählervergleichseinrichtung geschaltet und der Anschluß des Kunden wird so für einen bestimmten Zeitraum n a c h dem fraglichen Zeitraum doppelt überwacht. Diese Maßnahmen dienen letztlich dazu, den „Beweis des ersten Anscheins“ oder kurz „Anscheinsbeweis“ vorzubereiten.

Exkurs Anfang:

Was ist ein Anscheinsbeweis?

In unserem Rechtssystem muß - Gott sei Dank - immer derjenige, der von einem anderen etwas haben will (hier beispielsweise der Anbieter die Bezahlung einer überhöhten Rechnung) die Voraussetzungen dafür sowohl d a r l e g e n als auch b e w e i s e n. In bestimmten Fällen kann sich der Beweispflichtige (hier der Anbieter) dazu auf die Beweiserleichterung des Anscheinsbeweises berufen.

Diese Beweiserleichterung wurde von der Rechtsprechung entwickelt. Der Anscheinsbeweis kommt aber nur dann in Betracht, wenn ein Sachverhalt nach der „Lebenserfahrung“ (so nennen das die Juristen ;)) auf einen bestimmten, typischen Verlauf hinweist. Dann kann von einer feststehenden Ursache auf einen bestimmten Erfolg oder - umgekehrt - von einem feststehenden Erfolg auf eine bestimmte Ursache geschlossen werden. Er gilt also nur für typische Geschehensabläufe. (Bitte erst durchdenken!)

Beispiel: Wenn ein Dach kurz nach der Errichtung einstürzt, dann spricht der Anscheinsbeweis dafür, daß das Dach fehlerhaft errichtet wurde.

Damit könnte dann die Behauptung als bewiesen angesehen werden. Das gehört alles zur Beweiswürdigung, die das Gericht durchführt und bedeutet k e i n e Umkehr der Beweislast, sondern eben nur eine Erleichterung der Beweislast.

Ist der Kunde also hilflos ausgeliefert? Nein!

Er kann den Anscheinsbeweis entkräften, dann muß wieder der andere (hier der Anbieter) den vollen (strengen) Beweis für seine Behauptung erbringen (hier die in Rechnung gestellten Einheiten). Der Anscheinsbeweis ist entkräftet bzw. erschüttert, wenn der Gegner (hier der Kunde) Tatsachen behauptet und beweist, aus denen sich die e r n s t h a f t e Möglichkeit eines anderen Geschehensablaufs ergibt, wenn also etwas anderes e r n s t h a f t in Betracht kommt.

Exkurs Ende. -

Der Kunde kann dann verlangen, in diese Dokumentationen Einsicht zu nehmen („ist vorzulegen“). Einen Anspruch auf Aushändigung hat der Kunde nicht. Diese Regelung ist aber Unsinn, denn in einem Prozeß müssen Klageschrift und Beweismittel in dreifacher Ausfertigung eingereicht werden (für das Gericht im Original, für den Beklagten (Kunden) und für den Rechtsanwalt des Kunden). Deswegen sollte man auf diesen Umstand hinweisen, wenn eine Weigerung der Herausgabe dieser Dokumentation seitens des Anbieters erfolgt.

§ 16 Abs. 2: Ist klar, hier wird deutlich gemacht, daß der Kunde nichts Unmögliches verlangen kann. Wenn die Entgelterfassungsgeräte vom Blitz getroffen wurden oder der Kunde nicht möchte, daß seine Verbindungsdaten gespeichert werden, kann der Kunde sich eben auch auf § 16 Abs. 1 nicht berufen; was nicht da ist, kann auch nicht eingesehen werden.

verarschung (TKV)

Auszug aus der Telekommunikations-Kundenschutzverordnung (TKV)

§ 16 Nachweis der Entgeltforderungen

(1) Erhebt der Kunde bei Telekommunikationsdienstleistungen für die Öffentlichkeit, die auf den für die Sprachkommunikation für die Öffentlichkeit vorgesehenen Telekommunikationsnetzen erbracht werden, Einwendungen gegen die Höhe der ihm in Rechnung gestellten Verbindungsentgelte, so ist das Verbindungsaufkommen unter Wahrung des Schutzes der Mitbenutzer auch ohne Auftrag zur Erteilung eines Einzelentgeltnachweises nach den einzelnen Verbindungsdaten aufzuschlüsseln und eine technische Prüfung durchzuführen, deren Dokumentation dem Kunden auf Verlangen vorzulegen ist.

(2) Soweit aus technischen Gründen oder auf Wunsch des Kunden keine Verbindungsdaten gespeichert oder gespeicherte Verbindungsdaten auf Wunsch des Kunden oder auf Grund rechtlicher Verpflichtung gelöscht wurden, trifft den Anbieter keine Nachweispflicht für die Einzelverbindungen, wenn der Kunde in der Rechnung auf die nach den gesetzlichen Bestimmungen geltenden Fristen für die Löschung gespeicherter Verbindungsdaten in drucktechnisch deutlich gestalteter Form hingewiesen wurde. Soweit eine Speicherung aus technischen Gründen nicht erfolgt, entfällt die Nachweispflicht, wenn der Kunde vor der Rechnungserteilung auf diese Beschränkung der Möglichkeiten des Anschlusses in drucktechnisch deutlich gestalteter Form hingewiesen wurde.

(3) Dem Anbieter obliegt der Nachweis, die Leistung bis zu der Schnittstelle, an der der allgemeine Netzzugang dem Kunden bereitgestellt wird, technisch einwandfrei erbracht und richtig berechnet zu haben. Ergibt die technische Prüfung Mängel, die die beanstandete Entgeltermittlung beeinflußt haben könnten, wird widerleglich vermutet, daß die Verbindungsentgelte des Anbieters unrichtig ermittelt sind. Ist der Nachweis erbracht, daß der Netzzugang in vom Kunden nicht zu vertretendem Umfang genutzt wurde, oder rechtfertigen Tatsachen die Annahme, daß die Höhe der Verbindungsentgelte auf Manipulationen Dritter an öffentlichen Telekommunikations-netzen zurückzuführen ist, ist der Anbieter nicht berechtigt, die betreffenden Verbindungsentgelte vom Kunden zu fordern.

(vollständig auf http://www.regtp.de/Rechtsgrundlagen/TKV.htm)

Mehr bedeutet Abs. 2 nicht, insbesondere n i c h t , daß derjenige Kunde, der auf eine Speicherung der Verbindungsdaten verzichtet hat, jeglichen Rechtsschutz verliert.

§ 16 Abs. 3: Besteht aus drei Sätzen. Satz 1 ist der interessanteste. Mit „Schnittstelle des allgemeinen Netzzugangs“ kann ja wohl nur die TAE-Anschlußdose (analoge Leitung) oder der (das?) NT (digital bzw. ISDN Leitung) in der Wohnung des Kunden gemeint sein. Bei „Leistung“ handelt es sich um die duplexen Signalübertragungen (analog oder digital) bei einer Verbindung bzw. das Bereithalten der Möglichkeit, eine solche Verbindung herzustellen.

Störend ist dabei aber der Begriff „bis“ zur Schnittstelle. Soll das heißen „nur bis“ oder „auch bis“? Wenn nun jemand die „Leistung“ von der Vermittlungsstelle bis zur Wohnung des Kunden ganz oder teilweise induktiv oder galvanisch abgreift, hat dann der Anbieter die „Leistung“ „bis“ zur Wohnung des Kunden dennoch im Sinne von § 16 Abs. 3 Satz 1 erbracht?

Ist es denn überhaupt technisch möglich, zu erfassen, „bis“ wo hin ein elektrischer Strom fließt, ohne daß am Ziel ein Meßgerät installiert wurde? Die Tatsache allein, daß der Strom verbraucht wurde, bringt dazu ja wohl keine Erkenntnis, wo er denn wohl verbraucht wurde (beim Kunden oder beim unredlichen Dritten?).

Dazu ein Beispiel: Irgendwo auf der Strecke von der Vermittlungsstelle zur Wohnung des Kunden durchtrennt ein unredlicher Dritter die Leitung und versieht sie mit einer Steckverbindung. Bei Bedarf trennt er die Leitung

und telefoniert auf Kosten des Kunden, danach verbindet er die Leitung wieder.

Hier dürfte wohl klar sein, daß die Leistung eben nicht bis zur Wohnung des Kunden erbracht wurde. Wie aber will der Anbieter so seiner Beweispflicht nach Satz 1 nachkommen? Dies ließe sich nur durch einen manipulationssicheren Zähler an der Anschlußdose in der Wohnung des Kunden realisieren, vergleichbar mit den allseits bekannten Strom-, Gas- und Wasserzählern.

Wenn dieser Satz 1 richtig angewendet würde, wären auch die Sätze 2 und 3 überflüssig. Anhand deren Existenz ergibt sich aber, daß Abs. 3 DIE Mogelpackung der TKKuschVO überhaupt ist, denn beim Überfliegen des erstens Satzes drängt sich der Eindruck auf, der Anbieter müsse nunmehr nachweisen, daß sämtliche in Rechnung gesetzten Einheiten auch tatsächlich vom Kundenanschluß genutzt wurden. Jedoch muß Satz 1 auch immer im Zusammenhang mit den Sätzen 2 und 3 gelesen werden.

Tatsächlich gibt der § 16, insbesondere Satz 3, nur den bekannten Ablauf des Verfahrens wieder, der beim Beweis des ersten Anscheins angewendet wird. Die dort genannten „Tatsachen“ sind nichts weiter als die greifbaren Anhaltspunkte, die geeignet sind, den Anscheinsbeweis zu erschüttern.

Im Ergebnis hat sich also nichts geändert. Von Beweislastumkehr kann nicht die Rede sein. Nach wie vor muß der Kunde beweisen, daß der Netzzugang im vom Kunden nicht zu vertretendem Umfang genutzt wurde. Oder er muß Tatsachen beibringen, die die „Annahme rechtfertigen“, daß Manipulationen Dritter an den Netzen Einfluß auf die Höhe der Entgelte hatten. Der Anbieter braucht nach wie vor nur zu beweisen, daß richtig gerechnet wurde und alles technisch einwandfrei ablief. Dazu reichen dem Anbieter die technischen Protokolle und das Ergebnis der Zählervergleichseinrichtung sowie ein entsprechnd aufbereiteter, sachverständiger Vortrag eines technischen Angestellten des Anbieters vor Gericht.

Da die Richter - von wenigen Ausnahmen abgesehen - nicht über Grundkenntnisse der modernen Telekommunikation verfügen, wird hier immer noch viel zu voreilig der Anscheinsbeweis angenommen werden.

Ein mutiger Richter würde hier den Anscheinsbeweis nicht vorschnell zubilligen, sondern von § 16 Abs. 1 Satz 1 Gebrauch machen und dem Anbieter einen Hinweis geben, wonach dieser seine Behauptung (streng) beweisen muß, daß er seine Leistung „bis zur Anschlußdose“ des Kunden erbracht hat (falls er dazu nicht in der Lage sein sollte, wird er die Klage des Anbieters konsequenterweise abweisen).

Bernd Ruschinzik, beru@bln.de

<Rechtsanwalt bei der Verbraucherzentrale Berlin>

Gebührenimpuls strikes back

Nachdem es Anfang des Jahres ein zu einem kleinen Gebührenmalheur kam, als allgemein festgestellt wurde, daß es beim Telefonieren über die neuen Telefongesellschaften keinerlei Gebühreninformationen mehr gab (s. ServiceWatch vom 13.1.98 unter http://www.ccc.de/ServiceWatch/), einigten sich die neuen Wettbewerber und die Telekom Mitte Mai auf eine Zwischenlösung.

Der Gebührenimpuls (bei analog-Anschlüssen) bzw. das AOC-Paket (Advice Of Charge, bei ISDN-Anschlüssen) wird bisher jeweils in der lokalen Vermittlungsstelle des Anrufers erzeugt. Die Vermittlungsstelle entscheidet anhand von bis zu acht Ziffern der gewählten Rufnummer, wie oft (oder ob überhaupt) eine Gebühreninformation zum Teilnehmer geschickt wird. Um ein Übermitteln dieser Informationen von anderen Anbietern zu ermöglichen, müßten diese durch das Netz transportiert werden und nicht erst lokal anhand der Rufnummer erzeugt werden. Da diese Änderungen im SS7-Protokoll zwar vorgesehen sind, die ITU (http://www.itu.int) aber bekanntlich gemächlich arbeitet und die Implementation in die Software der Vermittlungsstellen auch ausführlich getestet werden will, ist mit einer grundsätzlichen Lösung erst in einigen Jahren zu rechnen.

Bis dahin will man sich mit dem alten Verfahren behelfen: Die Netzbetreibervorwahlen werden in die Verzonungsdatenbanken der Telekom-Vermittlungsstellen eingetragen und diese erzeugen dann wie gehabt lokal die Gebühreninformation. Das wird jedoch in einigen Problemen resultieren: Die T sendet jeweils für 12 Pfennig einen Gebührenimpuls (genauer gesagt für 12,1 Pfennig - da war ja noch die Sache mit der MwSt-Erhöhung). Die anderen Anbieter haben aber meistens gar kein Einheitenkonzept, sondern rechnen z.B. im Sekunden- oder Minutentakt ab. Deren Tarifstruktur wird dann also in das 12-Pfennig-Korsett gezwängt.

Des weiteren werten die Vermittlungsstellen bisher nur die ersten acht Ziffern der Rufnummer aus. Für normale Vorwahlen reicht das völlig. Wenn dann aber noch die Netzbetreiberkennzahl hinzukommt, kann es kritisch werden, insbesondere seit die zweistelligen alle sind und jetzt dreistellige vergeben werden. Ein Beispiel:

```
010xxx00
^  ^  ^
|  |  Auslandsgespräch
|  Netzbetreiberkennzahl
Call-by-Call
```

...und schon sind acht Ziffern belegt, und die VSt erkennt gerade nochmal, daß es sich um ein Auslandsgespräch über den gewählten Betreiber handelt, aber nicht, in welches Land es geht.

Der Gebührenimpuls wird also nach seiner Rückkehr im Herbst höchstens einen Anhaltspunkt über die anfallenden Kosten geben. Individuelle Rabattmodelle wurden sowieso noch nie berücksichtigt, auch innerhalb des T-Netzes nicht.

tobias@ccc.de

Unterrichtsblätter der Telekom auf CD-ROM

Die Unterrichtsblätter der Telekom - ein muß für jeden Phone-phreak mit Infodurst - des Jahres 1997 gibt es jetzt auf CD-ROM für 15.- DM (Volltext) für Windows und Apple Macintosh; einschl. Verpackung und Versand. Zu Bestellen durch Überweisung des Betrages auf Kto. 166191-662 bei der Postbank Saarbrücken (BLZ 59010066) der Unterrichtsblätter. Als Verwendungszweck der Überweisung „CD-ROM“ sowie vollständige Versandanschrift angeben. Sehr zu empfehlen.

Chaos Realitäts Dienst: Kurzmeldungen

Microsoft übernimmt Lehrstoffinhalte: 200 Dollar pro „Microsoft“

Laut einer Meldung der PC-Welt betreibt Microsoft derzeit eine Werbekampagne der ganz besonderen Art: Die Firma zahlt an College-Professoren 200 Dollar, wenn sie in einem Vortrag ein Microsoft-Produkt erwähnen. Die Professoren müssen die Erwähnung lediglich mit Hilfe eines Formulars dokumentieren und erhalten daraufhin einen Scheck.

Nach einem Bericht des Chronicle of Higher Education hält Microsoft dieses Verfahren nicht für eine Form der Bestechung, da es sich ja nur um geringe Beträge handle.

Vorzeitige Zementierung des Bundesdatenschutzbeauftragten Jakob

Rechtzeitig vor der Wahl wurde der Bundesbeauftragte Jakob von der Regierungs-mehrheit im Bundestag auch für die nächsten 5 Jahre wiedergewählt; damit ist das Wahlergebniss bei der nächsten Bundestagswahl im Bezug auf die Position des Bundes-datenschutzbeauftragten unerheblich. Für welche Verdienste Jakob von immerhin 562 Abgeordneten wiedergewählt wurde ist uns nicht bekannt; seine Verdienste in der Öffentlichkeit aufzutreten ohne dabei Unternehms- oder gar Behördenvertretern weh zu tun sind jedoch anerkennenswert. Ob dies die Position des Bundestdatenschutzbeauftragten ausmachen sollte, steht auf einem anderen Blatt.

Jakob hat sich dabei nicht nur der Initiative der Landesdatenschutzbeauftragten gegen den Lauschangriff verschränkt, sondern auch sonstige Beschlüsse des Innenministers wie der Einrichtung der Gendatei im Kern begrüßt.

Sicherheitskopien von CD-ROMs sind minder legal

Das Erstellen von Sicherheitskopien von CD-ROMs (einschliesslich Playstation) wurde jetzt vom Landgericht Bochum in einer Entscheidung Anfang Mai untersagt. Die einzige Ausnahme sind Kopien, die zur weiteren Nutzung des Originalprogramms notwenig sind. Das Urteil kam zustande, nachdem ein Verfahren gegen einen Softwarehersteller angestrengt war, der Sicherheitskopien von CD-ROMs als Serviceleistungen anbot. Im Hinblick darauf, dass Datenverluste auf einer CD-ROM äusserst selten aufträten und es unter wirtschaftlichen Gesichtspunkten nicht plausibel sei, eine Kopie zu erstellen, erschien es der Kammer zweifelhaft, ob solche Kopien tatsächlich der Datensicherung dienen.“

Mobiltelefonblockierer

Die israelische Firma Netline Technologie hat ein Mobilfunkstörgerät für klingelfreie Räume und sensitive Stellen (Handhabung vertraulicher Informationen) entwickelt.

In Arbeit befindet sich derzeit eine Weiterentwicklung, die es ermöglichen soll, daß wichtige Anrufe für bestimmte Mobiltelefone, deren Nummern zuvor eingegeben werden, den Schutzwall durchdringen können. „Man müsse allerdings sicherstellen, daß diese Technik nicht in die falschen Hände gerät, um unerwünschte Telefongespräche zu unterbinden oder Schäden zu verursachen.“ (aus: Heise-Ticker, neulich)

BND Abwicklung?!

Derzeit bekommt der BND derart öffentlich Feuer, daß man sich fragt, was da passiert.

Einfach nur draufprügeln wäre dumm, selbst dann, wenn es Spaß macht, weil man Geheimdienste ablehnt. Wird die Frührentnerversorgungsanstalt für Politiker in führungsähnlichen Positionen gerade abgewickelt? Wie geht das eigentlich mit dem Outsourcing von Recherchejobs bei diesen Diensten? Bekommt der CCC nach Abwicklung des BND dessen Spielzeuge geschenkt? Zumindest an den DES-Knackmaschinen besteht durchaus Interesse. Zudem ist es ein gesellschaftliches Problem, wenn ein Geheimdienst abgewickelt wird. Denn was danach kommt, ist in einer demokratischen Gesellschaft womöglich noch schwerer zu kontrollieren als der finstere Istzustand.

Unklarer Indischer Atomhack

de.org.ccc-Leser wissen vom indischen Atomhack. Da wurden US-Militärrechner aufgemacht und mit dem Bitbohrer von einem Zahnarztsystem aus ging es weiter. Letztlich wurde ein Atomforschungszentrum in Indien aufgebohrt und abgesaugt. Dann wurde das ganze mit einer neu gestalteten Anti-Atom-Seite im WWW verplombt. Respekt für den Mut; das ist schon etwas mehr als ein einfaches Web-Graffiti, also das Umfärben einer Webseite anstatt einer Häuserwand. Es ist schon eine harte Nummer, wenn von US-Militärrechnern aus ein indisches Atomforschungszentrum aufgemacht wird. Unklar war, was in Istanbul bei Atomforschungszentren alles passierte. Aber da sind die USA wohl selbst recht zurückhaltend.

Grenzen des Hackens

Grenzen des Hackens wurden aus Kreisen der 2600 berichtet. Da hatte einer sich durch die Instanzen durchgefragt, ob den das Hacken von Computern im Ausland verboten sei. Auf jeder Ebene hörte er ein Nein, er möge das zwar bitte unterlassen, aber verboten sei es nicht. Nachdem er jedoch ein paar französische „Groß-Dosen“ öffnete, kam eine diplomatische Note beim State-Department an: das Hacken sähe Frankreich als „Act of War“ (Kriegsakt). Daraufhin waren die so freundlich, den Hacker durch sofortigen

Hausbesuch auf Probleme hinzuweisen, die manchmal mit Büchsenöffnen verbunden sind.

Hagbards Todestag

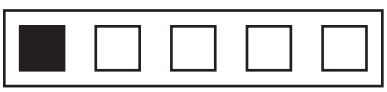
Am 23. Mai 1989 kam Hagbard zu Tode. Auch wenn Hacker nicht zur Spezies der besonders Sentimentalen gehören, ist der 23.5. für viele ein Tag der Erinnerung an einen lieben Menschen. Und daß ein Mensch nicht nur Stärken hat, ist normal - immerhin hat sogar der Verfassungsrechtler Benda ein „Grundrecht auf Fehler“ festgestellt. Der CCC hat die Dokumentation zu Hagbard gescannt, in verschiedenen Auflösungen unter ftp://www.ccc.de abrufbar.

Wusstet ihr schon...

...daß die Telekom zur Anbindung der HIT-Nets an das Internet die Altavista Firewall 3.0 mit immerhin 56 Bit DES-verschlüsseltem Administrationszugang benutzt?

...daß Quicken 98 „aus Sicherheitsgründen“ nur noch numerische und nicht mehr wie vorher alphanumerische PIN´s benutzt ?!

...was die Bundesstelle für Fernmeldestatistik mit dem inländischen Telefonverkehr der letzten 24 Monate im Lastenausgleichsverfahren treibt?



GSM: Security by obscurity

Wie die Datenschleuder berichtete, hatte sich das GSM MoU (Memorandum of Understanding, ein Industriekonsortium, das den GSM-Standard entwickelt und vorantreibt) entschlossen, die für die Authentifizierung und Verschlüsselung im GSM verwendeten Algorithmen geheimzuhalten. Der für die Verschlüsselung verwendete Algorithmus A5 ist (in zwei Varianten, A5/1 mit ein bisschen Sicherheit, A5/2 mit noch weniger Sicherheit) bei allen Netzwerken und Telefonen im GSM identisch, eine fast korrekte Implementation kursiert seit Jahren im Internet.

Für die Authentifizierung und die Festlegung des Session-Keys für die Luftschnittstellen-Verschlüsselung werden die Algorithmen A3 und A8 verwendet. Das GSM MoU hat sich dabei nicht auf einen Algorithmus festgelegt, es steht jedem Hersteller frei, eine eigene Implementation zu verwenden. Interoperabilität ist nicht notwendig, da sich auch beim Roaming alle verschlüsselungsrelevanten Vorgänge entweder auf der Chipkarte oder im HLR des Netzbetreibers abspielen, der die Karte ausgegeben hat.

Jetzt begab es sich aber, dass das MoU eine Referenzimplementation von A3/A8 namens COMP128 für seine Mitglieder bereitstellte. Das führte dazu, dass eine Vielzahl von Netzwerk-Operatoren diesen Algorithmus ungeprüft einsetzte, da sie davon ausgingen, das MoU wisse schon, was es da tut.

Wusste es aber nicht. Da COMP128 nie veröffentlich wurde, gab es keine unabhängige Sicherheitsüberprüfung durch außenstehende Kryptografen, wie sie bei allen heute gängigen Algorithmen wie RSA, IDEA oder Blowfish durchgeführt wurde. Ein Algorithmus gilt dann als relativ sicher, wenn er mehrere Jahre veröffentlich ist und niemand eine praktische oder realistisch erscheinende theoretische Attacke veröffentlicht hat.

Und es begab sich, daß der Smart Card Developer Association (http://www.scard.org) ein Satz von Schulungsunterlagen in die Hände fiel, in dem COMP128 größtenteils erklärt wurde. In diesen Schulungsunterlagen gab es einige offenkundige Weglassungen und Fehlinformationen, die durch „manuelle“ Forschung identifiziert und berichtigt werden konnten. Durch längeres Studieren einer GSM-Testkarte, bei der der geheime Schlüssel Ki frei gewählt werden konnte, wurden die restlichen Details rekonstruiert.

Marc Briceno von der SDA hat die Sourcen des COMP128 dann an Ian Goldberg und Dave Wagner geschickt. Die beiden bilden das Kernteam einer Sicherheitsforschungsgruppe an der Uni in Berkeley. Und sie haben dann auch nach nur sehr kurzer Zeit eine Sicherheitslücke in COMP128 entdeckt.

Das Problem ist, daß es beim COMP128 verschiedene Inputs gibt, die denselben Output erzeugen, sogenannte Kollisionen. Diese Kollisionen treten bereits nach der zweiten Runde der Berechnung auf. Zu diesem Zeitpunkt sind die Bits des Inputs noch nicht besonders gut über den gesamten Buffer verteilt, was zur Folge hat, dass diese Kollisionen nur von 32 der insgesamt 256 Input-Bits abhängig sind.

Der Input von COMP128 sind 16 Byte Challenge-Daten vom Netz (RAND), und 16 Byte geheimer Schlüssel (Ki) in der Karte. Die 32 Bit, die für die Kollision entscheidend sind, sind jeweils das i-te und i+8-te Byte von RAND und Ki.

Der erste Schritt, um den Ki aus der Karte zu extrahieren, ist jetzt, Kollisionen zu finden. Ki kann man naturgemäß nicht variieren, RAND jedoch schon. Man nimmt jetzt also die Karte, wählt sich einen RAND, schickt RAND an die Karte, und schaut dann in einer Tabelle nach, ob man die Antwort schon gesehen hat.

Da die Kollision ja nur von 2 Bytes in RAND abhängig ist, ist es egal, wie der Rest der Bytes von RAND aussieht, wir setzen also alles auf 0, ausser den Bytes, in denen uns die Kollision interessiert. Wenn wir mit i=0 anfangen, zählen wir jetzt alle Kombinationen von Byte 0 und Byte 8 von RAND durch, bis wir ein Paar von RAND-Werten mit einer Kollision finden. Da die Kollision ja nur von Bytes 0 und 8 von Ki abhängig ist, können wir jetzt in einer Simulation der Karte (einer Software, die den COMP128 enthält), beginnend mit einem Ki von 0, alle Werte von Byte 0 und 8 durchprobieren, bis wir mit diesem Ki eine Kollision für dasselbe Paar von RANDs wie bei der Karte sehen.

Und schon haben wir 16 Bit von Ki. Durch Wiederholen dieses Prozesses für i von 1 bis 7 können wir den gesamten Key rekonstruieren.

Notwendig für diesen Prozeß ist natürlich ein Kartenleser, eine Software, die eine Anfrage an die SIM-Karte schickt, und eine COMP128-Implementation, um die Keys durchzuprobieren. Einen Linux-Source für das entsprechende Programm, der mit dem UniProg oder dem Dumbmouse-Interface läuft, gibt's auf ftp://www.ccc.de.

Der Zeitaufwand zur Extraktion des Ki hängt massiv von der Geschwindigkeit ab, mit der die Karte die Challenges abarbeitet. Erfahrungsgemäß zieht sich das ganze etwa acht Stunden hin, gelgentlich auch länger. Durch einige Optimierung im Ablauf und elektronische Massnahmen dürfte eine deutliche Reduzierung dieser Zeit möglich sein.

andreas@ccc.de / frank@ccc.de

CCTV Systeme: Kameraüberwachung

Im Rahmen der „Nordischen Sicherheitstage“ in Lübeck berichtete Derrick Scougal von der Polizei in Newcastle (GB) über die Einführung und Erfahrungen von Videoüberwachungen öffentlich zugänglicher Bereiche.

Ausschlaggebend für die Installation des Systems war 1985 ein „Football Disorder“ in dessen Verlauf nicht nur ein Teil der Innenstadt, sondern auch der Polizeikräfte demoliert wurden. Ein weiterer Grund, warum Newcastle als Referenzimplementation auserkoren wurde lag am „Roundrading“ Rekord in dieser Region. Bei Roundrading handelt es sich um eine offenbar Mitte der 80er Jahre vor allem in England verbreitete Sportart, die in mehreren Etappen verläuft. Zunächst wird ein beliebiges, aber robustes Auto geklaut. Mit diesem Auto wird dann - zum Zwecke des ausraubens - in ein Geschäft (also z.b. einen Juwelier) hineingefahren. Unter hineinfahren ist dabei die frontale Einfahrt in das Schaufenster zu verstehen. Die letzte Etappe - nach dem ausrauben - verläuft dann in verschiedenen möglichen Varianten. Entweder die Sportler ...äh Täter... flüchten zu Fuss, oder aber mit diesem oder einem anderen Auto.

Das erste installierte System umfaßte 16 Kameras und kostete rund 300.000 Pfund (fast ne Mio. DM). Die Kameras sind dabei grundsätzlich mit Infrarotscheinwerfern ausgerüstet und können von der Ferne vollständing gesteuert werden („zooming & dancing“). Die Überwachungszentrale wird von der Polizei betrieben und ist 24 Stunden am Tag besetzt; die Kameras sind in der Regel in „Problembereichen“ (Nachtclubs, Fußgängerzonen u.ä.) installiert und grundsätzlich gedoppelt (also 8 Bereiche); dadurch ist es möglich, Verdächtige von vorne wie von hinten zu beobachten (front & back) bzw. Unmöglich sich als Verdächtiger durch umdrehen der Beobachtung zu entziehen (Drogenhändler). Von Verdächtigen können in der Überwachungszentrale kurzfristig Hardcopys der Bildschirmfotos gemacht. Diese wurden in der Anfangszeit noch manuel entsprechenden Greiftrupps („go find that man“; roboterisierbare Bluthundfunktion) in die Hand gedrückt. Mittlerweile gibt es eine einfache Funkfaxübertragung zu den Streifenwagen um den Zeitfaktor zu verbessern.

Insgesamt sind in der Innenstadt von Newcastle allerdings 600 Kameras installiert, in der Regel von Geschäften, Läden aber auch privaten Sicherheitsfirmen. Die Polizei verfügt durch entsprechende Datensammelaktionen über eine Datenbank mit allen Kameras, ihren Blickwinkeln, Betreibern, Art der Aufzeichnung etc. - die Datenbank wurde leider nicht gezeigt. Um die Effektivität dieser Datenbank zu veranschaulichen (und bei der Gelegenheit natürlich gleich kritische Zielgruppen zu beeinflußen) erzählt Scougal von der Vergewaltigung einer jungen Frau, die vor der eigentlichen Tat eine halbe Stunde vom Täter quer durch die Innenstadt verfolgt wurde. Die Aufzeichnungen der Polizeikameras waren dabei wenig hilfreich, da sie zwar einmal die junge Frau, nicht aber den Täter aufzeichneten. Da die Frau allerdings die Strecke recht gut errinerte, konnte die Polizei über die Datenbank sich die Aufzeichnungen der Kamerasysteme entlang des Weges besorgen; der Täter konnte somit ermittelt, überführt und für 9 Jahre ins Gefängniss gesteckt werden. Zukünftig soll die manuelle Verfolgung von „target criminals“ automatisiert werden; auch sind weitere Arbeitsplätze für die Anlegen von Verdächtigenkarteien / Datenbanken in Plannung. Die Überwachungsräume sollen dabei noch mit Sofas und Refreshments (was auch immer das in der Sprache eines Polizisten heißt) ausgestattet werden, um sie als Aufenthaltsraum mit gleichzeitigen Beobachtungen zu nutzen.

Auch andere Formen der Bildverwertung wurden schon erfolgreich durchgeführt; so wurden mehrere Anzeigenkampagnen geschaltet, in denen die Bilder von Randalierern nach einem Fussballspiel zusammen mit einer „0130-Denunziationsnummer“ abgedruckt wurden; der

öffentlicher Orte

Rücklauf war zufriedenstellend; oft meldeten sich die Gesuchten selbst, weil sie am Arbeitsplatz z.B. auf Ihr Foto in der Zeitung angesprochen worden waren. Um das System auszubauen, ist in Newcastle jetzt eine Einrichungspauschale bei Erwerb einer Gaststätten- / Diskotheken- / Nachtclub-konzession eingeführt worden; nach dem „Verursacherprinzip“ seien das ja schließlich Unruheherde, die überwacht werden müssten und entsprechende Kosten verursachen.

Von gesellschaftlichen Empfindlichkeiten weiß man von Betreiberseite in diesem Land wenig. Daß durch Aufmerksamkeitsvermarktung erzeugte Unsicherheitsgefühl (Medienhype Kindermord etc.) ist fortgeschritten, daß Kameras ein Sicherheitsgefühl vermitteln. Wenn sich die Medien in Deutschland so weiterentwickeln, ist die Bevölkerung hier allerdings auch bald empfänglich für den Schutz durch den großen Bruder. Auf das Thema Denunziationsgesellschaft angesprochen, kam ansatzweise Zustimmung von einigen anwesenden Zivilisten. Anwesende Staatsbedien-stete in Uniform mussten sich erst noch die Tränen der Begeisterung aus den Augen wischen.

Problematisch fand der Referent allenfalls den Mißbrauch des Filmmaterials bei den Medien; die würden „very cheap“ daraus „crime watch tv“ machen. Auch seien viele Systeme im Internet verfügbar. Die Empfindlichkeiten, für einen Überwachungsstaat nützliche Technologie jetzt schon zu installieren, scheinen am schwinden.

Für weitere Informationen nehmt euch Zeit und fragt Altavista nach: CCTV

andy@ccc.de

Zum Titelbild:

Komprimitierende Emission (KEM) ist in der Hackerszene noch viel zu wenig besprochen worden. Gut, daß ist Geheimdienstwerkzeug - aber Geldautomaten werden damit schon länger leergemacht. Zu Titelbild und untigem Text gibt es zur Abwechselung mal keine Quellenangabe. Wir suchen noch jemanden, der sich mit KEM schon näher beschäftigt hat und etwas für die Datenschleuder schreiben mag. Die meisten fitten Leute in der Branche haben da so Verbindlichkeiten...

Die Formen des Angriffes sind unterschiedlich.
Am Beispiel der Abhörung eines Geldautomatens ist es nicht wichtig das Graphiksystem zu belauschen, sondern Ziel der Aktion sind die Emissionen der Tastatur und des Geldkartenlesegerätes. Mit diesen Informationen stehen dem Angreifer der Pincode und die auf der Karte abgelegten Daten zur Verfügung. Daten, die zur Prüfung und zur Geldauszahlung benötigt werden.
Der Angreifer muß seine Antennenschleife nicht weiter als 8 Meter entfernt installieren, z.B. in einem benachbarten Treppenhaus oder angrenzenden Raum, der nicht im Sicherheitsbereich der Bank liegt.
Da es sich um nichtrepetierliche Signale handelt, müssen sie aufgezeichnet werden. Als Aufzeichnungsgerät reicht neben dem Empfänger ein modifizierter Kassettenrecorder / Diktiergerät. Anschließend erfolgt die Bearbeitung der gesammelten Daten im offline-Verfahren in den eigenen vier Wänden.

SSL Attacke

In den letzten Tagen ging eine SSL-Attacke durch die Presse. Die Kurzzusammenfassung ist, daß das dem SSL-Protokoll zugrundeliegende PKCS1-Protokoll von RSA, Inc. ein Padding definiert, über die eine Chosen Plaintext Attacke lanciert werden kann.

Aber der Reihe nach.

PKCS1 ist der Public Key Cryptography Standard #1. So nennt RSA großspurig ihre eigenen Standards. Darin wird eine ganze Sammlung von Verschlüsselungsverfahren definiert, eine Protokoll-Suite sozusagen. Natürlich besteht diese praktisch ausschließlich aus RSA-Produkten.

Unter anderem definiert PKCS1 auch ein Protokoll zum Schlüsselaustausch. Krypto-Protokolle basieren meistens auf asymmetrischen und symmetrischen Verschlüsselung, wobei man der Geschwindigkeit wegen ein symmetrisches Verfahren mit einem zufällig generierten Schlüssel (genannt „Session Key“) benutzt, und diesen mit der langsameren asymmetrischen Verschlüsselung austauscht. Der Punkt dabei ist, daß man zum Entschlüsseln einer geheimen Nachricht nicht den privaten Schlüssel des Servers knacken muß, sondern es reicht, diesen Schlüssel für das innere, symmetrische Verfahren zu bekommen. Dieser ist aber zufällig gewählt und geht nur verschlüsselt über das Netz, und bei einer Schlüssellänge von 128 Bit kann heute und in absehbarer Zeit niemand einen Schlüssel erraten, indem er alle Möglichkeiten ausprobiert, weil das zu lange dauern würde.

Der Total-Angriff auf SSL2 wäre, den privaten Server-Schlüssel zu klauen, weil man dann die komplette Kommunikation abhören kann. Der von Bleichenbacher beschriebene Angriff geht aber nicht so weit, sondern er kann nur einen Session Key herausfinden, und damit eine einzelne Nachricht entschlüsseln.

Der Angriffspunkt ist der Schlüsselaustausch, der bei SSL aber nicht bei S/MIME oder SET oder anderen PKCS1-Protokollen auftritt. Die Idee ist, daß PKCS1 einige Felder definiert, bei denen nicht alle Möglichkeiten vergeben sind.

Der Angriff besteht jetzt daraus, daß manche Server zuerst das Padding überprüfen, bevor sie schauen, ob die Message überhaupt korrekt entschlüsselt werden konnte. SSL sieht auch eine MAC-basierte Validierung vor, anhand derer man später entscheiden kann, ob die Nachricht korrekt ankam. PKCS1 sieht vor, daß RSA-Nachrichten mit

0x00 0x02 0x??{8,n-m-3} 0x00 0x??{m}

anfangen. Die Attacke baut jetzt n Verbindungen zum Server auf. Bei SSL wählt der Client den Session Key aus und teilt ihn dem Server mit dessen öffentlichem Schlüssel (den der Server mitschickt) verschlüsselt mit. Der Angreifer kann jetzt Aussagen über den Session

Key machen, indem er Verbindungen aufbaut, die geratene Session Keys

hinschicken. Theoretisch müßte der Angreifer alle 128 Bit durchprobieren und schauen, ob das beobachtete Paket herauskommt, wenn er es mit dem public Key des Servers verschlüsselt. Nun hat RSA aber die Eigenschaft, daß man einen Cyphertext komplett entschlüsseln kann, wenn man einige Bits vorhersagen kann. Wenn man jetzt ein ungültiges Paket hinschickt, bei dem aber die beiden festen Bytes am Anfang stimmen, und der Webserver dann eine andere Fehlermeldung als „padding kaputt" zurückliefert, weiß man, daß die ersten beiden Bytes des Plaintextes 0x00 0x02 waren. Der Angreifer kann also manche Bits des Plaintexts bei chosen ciphertext (die Pakete, die er hinschickt) vorhersagen und ist damit ein informationstheoretisches Orakel. Das reicht, um den Plaintext komplett zu recovern.

Das Problem ist also, daß man gute Ciphertexte viel wahrscheinlicher generieren kann, wenn man schonmal einen guten hat. Den ersten kriegt man aber nur durch Ausprobieren. Bei der momentanen PKCS1 Implementation liegen die Chancen, einen guten zu raten, bei 1:2^16 bis 1:2^18. Ein Ciphertext ist gut, wenn er 0x00 0x02 am Anfang generiert beim Entschlüsseln.

RSA gibt an, daß man ungefähr 20 Millionen Fake-Nachrichten an den Server schicken muß, um den Session-Key der einen mitgelauschten Verbindung zu bekommen und damit die Verbindung entschlüsseln zu können. Praktisch gesehen ist die Attacke damit keine sonderliche Bedrohung, aber man sollte natürlich trotzdem etwas dagegen unternehmen. Wenn jemand gegen einen Web-Server diese Attacke fährt, sammeln sich etwa 300 Megabyte im Fehler-Log mit Meldungen, die einen falsches Padding andeuten. Für einen Webmaster ist also ziemlich klar, wenn sein Server unter Attacke ist, weil die Logs die Platte zum Überquellen bringen. Es bleibt noch, anzumerken, daß eine erfolgreiche Attacke dieser Art nur diesen einen Session Key kompromittiert, und bei späteren Attacken gar nicht hilft.

Der Fix ist natürlich ziemlich trivial: man prüft die Padding-Konsistenz erst, wenn die MAC gestimmt hat. Unter diesen Umständen ist nicht direkt einsehbar, wieso IBM eine Fix-Zeit von einer ganzen Woche angekündigt hat für ihren SSL-Webserver.

Leider gelang es mir nicht, das tatsächliche Paper zu finden. In Umlauf gebracht wurde das Problem von einer Rundmail der Firma C2, die die Käufer des Stronghold SSL-Servers gewarnt hat, sie mögen bitte updaten. C2 ist von RSA kontaktiert worden, die von Bleichenbacher offenbar direkt angesprochen wurden.

RSA hat inzwischen ein Bulletin 7 herausgegeben auf ihrer Website bei

http://www.rsa.com/rsalabs/pkcs1/bulletin7.html.

Felix von Leitner, felix@ccc.de

Krypto for the masses

Nach dem üblichen Gewese und anderweitig beschäftigt sein, ist im CCC die Krypto-Kampagne ausgebrochen. Nach und nach wird versucht werden, alle Kommunikation durch gesicherte Verbindungen zu piepen. An Dienstagen klappt das verschlüsseln ja manchmal schon genial, jetzt soll halt auch der Rest für nicht Angesprochene unverständlich ausgedrückt werden.

Das größte Problem, das Verschlüsselung bis jetzt hatte, war die nicht DAU Festigkeit der benötigten Programme. Das ist mit SSL und PGP in seiner neusten Version behoben. Die Bedienung und Konfiguration ist mittlerweile auf klicken reduziert, was es ermöglicht gesicherte Verbindungen als default zu setzen, ohne sich dem Vorwurf der Kommunikationsverhinderung auszusetzen. Was jetzt noch fehlt ist ein zumindest rudimentäres Verständnis der verwendeten Technik in größeren Teilen der Bevölkerung, insbesondere da Regierungen im eCommerce-Wahn versuchen, Techniken zu reglementieren, bevor sie von vielen Menschen soweit verstanden wurden, um eine demokratische Meinungsbildung zu ermöglichen.

Den Anfang der Krypto-Kampagne macht der Webserver, der seit Ende letzten Monats auch per https zu empfangen ist. Eine kurze Einführung in die Technik von SSL, zusammen mit den Links auf das verwendete CA-Cert findet sich auf dem unverschlüsselten Teil von www.ccc.de. Nach einer Eingewöhnungsphase wird der Zugang zum unverschlüsselten Teil (außer der Einführung) für SSL-fähige Browser verhindert.

Geplant ist weiterhin eine interne Domain einzurichten, auf die nur über SSL mit min. 128 Bit in Kombination mit Client-Certs zugegriffen werden kann und die Verschlüsselung der internen Mailinglisten. Soviel zur Zukunft, welche rosig, denn alles wird Gut.

Abhören und das Verhindern von Kommunikation war mit Papier basierter Kommunikation teuer und aufwendig. Das wird sich radikal ändern, wenn mehr und mehr des täglichen Gedankenaustausches in einer Form vorliegen, die automatisiert und kostensparend, kontrolliert und verhindert werden kann. Die politische Arbeit dies zu verhindern ist wichtig und funktioniert, siehe TkÜV, reicht allein aber nicht aus, denn solange es Gesetze gibt die Worte mit Strafe belegen, wird versucht werden die Verantwortlichen für diese Worte zur Rechenschaft zu ziehen und zu verhindern, daß andere diese Worte hören.

Das technische Probleme bis jetzt verhindert haben, bestimmte Angebote des Internet zu sperren, heißt nicht, das dies niemals gehen wird. Der erste mir bekannte automatische Newsscanner nach verbotenen Inhalten ist laut Zeitungsberichten am DE-CIX in Betrieb und einem Ausbau dieser Technik steht politisch nichts im Wege. Die NSA hört eh` alles und Bewertungssysteme für Inhalt à la Pics oder Cybernanny sind seit Jahren in Arbeit und es ist durchaus vorstellbar, daß es Provider geben wird, die ``sauberes', sprich gefiltertes Internet verkaufen. Was noch der angenehmste Fall wäre, den nach dem Urteil gegen Somm, könnte man sich auch Urteile gegen Provider vorstellen, die Dateien mit unerwünschten Bewertungen durchlassen. Die Gendatenbank läuft auch, es wird nicht grade besser mit der Freiheit in diesem Land. Als Begründung für diese Verschärfungen müssen Kinder herhalten, die eh` schon nichts zu lachen haben. In den USA sind's halt die Drogendealer, und anderswo ist es der dortige, derzeitige Staatsfeind Nummer Eins.

Es gilt also zu verhindern, daß Kommunikation beobachtet wird, denn erst aus dieser Beobachtung kann sich die Entscheidung, welche Inhalte gesperrt werden sollen, ergeben. Und genau aus diesem Grund ist es wichtig, daß nicht

nur sensible Daten verschlüsselt werden, sondern der ganze Traffic. Nach Möglichkeit auch mit einer Verschleierung der Verbindungsdaten.

Das alte Argument, daß wenn nur einer verschlüsselt, dieser eine prophylaktisch verhaftet wird, gilt weiterhin. Und könnte im Zuge der EU Harmonisierung Realität werden. Für die Verschlüsselung von Mailinglisten sprechen alle diese

Argumente. Und das das DoJ ≤ nach einem Bericht in der c't ≤ die internen Mails von Kleinweich abgehört hat und in einem Prozeß verwenden wird, ist zwar eine nette Anekdote, sollte aber Warnung genug sein.

Noch kurz zu dem Argument, daß eine weite Verbreitung von Krypto diese aufweichen würde, weil jetzt DAUs mit PGP spielen und die Keyserver irgendwann unbrauchbar werden etc. Jedem, der sich über diese Anfangsprobleme erhaben fühlt, steht es frei, seinen eigenen Keyserver aufzumachen und seinen Key täglich zu wechseln. Was verhindert werden sollte sind Lösungen, die Sicherheit vorgaukeln, ohne ihren

Versprechungen gerecht zu werden, aber solange dies erfüllt ist, ist gegen Krypto for the masses nichts einzuwenden. IMHO.

euer
Pluto

Krypto-Kurzmeldungen

Britanniens Tony greift nach dem Key
Europas Volksvertreter hören die Signale

London (CZ 07.05.9899 - Die britische Regierung will Strafverfolgern den Zugriff auf verschlüsselte Informationen ermöglichen. Bestimmte Kryptographieverfahren schreibt das geplante Gesetz nicht vor.

Die Blair-Administration plane die staatliche Lizenzierung von Kryptographiedienstleistern wie Zertifizierungsstellen und Key Recovery Agents, erklärte die Unterstaatssekretärin im Wirtschaftsministerium Barbara Roche in ihrer

Antwort auf eine parlamentarische Anfrage. Ähnliche Absichten der Major-Regierung waren einst auf den Widerstand der Industrie gestoßen. Deshalb will das Blair-Kabinett denn auch nicht vorschreiben, die Dienste der neuen Institutionen in Anspruch zu nehmen. Das Zugriffsrecht des Staates auf alle verwendeten Schlüssel, seien sie lizenziert oder nicht, soll in dem geplanten Gesetz allerdings verbrieft werden. **Achim Killer, Die Computerzeitung**

Übersicht Kryptoreglementierungen weltweit:

`http://cwis.kub.nl/~frw/people/koops/bertjaap.htm`

Single point of failure

Komplexe Systeme erzeugen komplexe Fehler. Zentralisierte komplexe Systeme erzeugen im Fehlerfall kleine Katastrophen.

Der Ausfall des Kommunikationssatelliten Galaxy IV am 05. Mai diesen Jahres, der PanAmSat Hughes, der größten amerikanischen Satellitenbetreiberfirma gehört, war in seinen Auswirkungen bislang einzigartig. Galaxy IV transportierte zu Lebzeiten neben einigen Übertragungskanälen für Fernsehüberspielungen und diversen landesweiten Radioprogramme die Daten für alle größeren Pagernetze in den USA. Pager (hierzulande untern den Namen Cityruf, Scall, Quix, Telmi oder Skyper bekannt) haben in Nordamerika eine wesentlich größere Bedeutung als in Europa. Da in den meisten Mobiltelefonnetzen der USA der Teilnehmer auch für ankommende Anrufezahlt, ist es üblich das Mobiltelefon ausgeschaltet zu haben und sich über einen Pager über Kommunikationswünsche benachrichtigen zu lassen. Viele Amerikaner benutzen ihren Pager auch als einziges Mobilkommunikationsmittel, insbesondere wenn sie in Bereitschaftsberufen, etwa als Arzt oder Feuerwehrmann, arbeiten. Da die Landfläche der USA relativ groß ist, wäre eine Versorgung der Sender des Pagernetzes mit den Daten zur Aus-sendung über Kabel recht kostspielig. Deshalb werden dort schon sehr lange die Daten von der Zentrale zu den Sendern per Satellit verteilt. Der meistgenutzte Satellit für diesen Zweck war nun Galaxy IV. Dies hatte einerseits mit der dafür besonders geeigneten Kanalstruktur der Transponder und andererseits mit der nahezu idealen Ausleuchtzone des Satelliten zu tun. Von dem Blackout waren nach Schätzungen etwa 45 Millionen Pagerkunden betroffen. Der Ausfall wurde, wenn man den Erklärungen von PanAmSat glauben darf, durch die Fehlfunktion des zentralen Steuerrechners und das Versagen des Backupsystems asugelöst. Der Satellit reagierte nicht mehr auf Korrekturkommandos von der Erde und drehte die Antennen aus der Erdrichtung. Hektische Versuche den Satelliten wieder unter Kontrolle zu bringen, führten zu keinem Ergebniss, außer der wenig hilfreichen Erkentniss, daß das wertvolle Gerät sich in einem „Safe State“ befinde. Für nicht mit der sensiblen Wortwahl der Raumfahrtingeneure vertraute Mitmenschen: er hat sich in eine Art Tiefschlafmodus begeben, bei dem es ziemlich unwahrscheinlich ist, daß er von selbst wieder aufwacht. PanAmSat entschied sich nach etlichen kostspieligen Stunden, nicht mehr auf eine Wiederherstellung der Kommunikation mit dem Satelliten zu hoffen und Notfallpläne einzuleiten. Kunden von Nachrichtenagenturen und Börsenin-formationssystemen wurden auf andere Satelliten, Kurzwellenaussendungen und sogar Internetlinks umgestellt. Radiosender, die ihre Nachrichten von Fremdanbietern wie landesweiten öffentlichen Rundfunksendern beziehen, besorgten sich die Texte oder sogar die gesprochenen Beiträge übers Internet. Die Pageranbieter begannen irgendwie Backup-Verbindungen zu den Sendern in den Ballungszentren hochzubringen und mit der Neuausrichtung der Satellitenschüsseln auf Ersatzsatelliten zu beginnen. Nach einigen Tagen waren alle Systeme wieder in einem Zustand, der als „Normal“ betrachtet wird. Das technisch wie verschwörungstheoretisch interessante am Galaxy IV-Ausfall ist, daß es bereits der dritte Satellit in Serie war, bei dem ein Ausfall der Kommunikationsverbindung zur Kontrolle der Flugbewegungen zu einem Totalverlust führte. Zuvor waren Indiasat (der wichtigste Satellit für Indien) und Earlybird1 (der erste wirklich hochauflösende kommerzielle Erdbeobachtungs-satellit) auf diese Art verloren gegangen.In diesem Zusammenhang bekommen die Gerüchte, wonach aus dem Wrack eines zivilen US-amerikanischen Kommunikationssatel-liten, der beim Abschuß mit einer chinesischen Rakete abstürzte, zentrale Baugruppen für die Verschlüsselung der Kontrolkommunikation fehlten, eine ganz unerwartete Brisanz.Probleme der „natürlichen“ Art mit Satelliten werden sich möglicherweise in den nächsten zwei Jahren häufen, da ein Sonnenfleckenmaximum ansteht (das in der Regel zu Beeinträchtigungen aller Art in der Umlaufbahn und im Funkverkehr führt) und der Meteoritenschwarm der Leoniden demnächst die Erdbahn kreuzt.

frank@ccc.de

Widerspruch willkommen

Bayerisches Gericht: Im Internet nur gottesfürchtige Bits

Spötter sprechen von der Übernahme Bayerns durch Microsoft, wenn Ende 1998 die Förderung bei Bayerns Bürgernetzen ausläuft und einiges „anders“ wird. Hacker lästern, der Umstieg auf Micro-Software und Active X bringt der bayrischen Justiz das ultimative Desaster. Denn bisher ist die Durchsetzbarkeit von Zugangsbeschränkungen im Internet nur unmöglich. Doch bei M$-Software halten Sicherheitslöcher einfach länger. Denn bei staatsfrommen und gottesfürchtigen Softwareanbetern ist die DAUer zum Begreifen größer als ein DAU braucht, um zu begreifen, daß die Erde keine Scheibe ist. Deshalb kommt man bei diesen Datenverkehrskreisen einfach länger mit althergebrachten Zugriffsmethoden an die Bithalden. Das nennt man dann Aufwärtskompatibilität. Das AT mit „Bit um Bit“ bei Datenangeboten im Internet gilt also weiter, auch wenn Jesus Christus mit dem NT ein Update mit integrierter Verzeihung auf den religiösen Geistermarkt brachte. Doch statt ein Katholische Kirchen Kombinat zu gründen, in dem nur die „guten“ Gläubigen Online sind, sollen die alttestamentarischen Regeln in der ganzen Welt gelten. Diese Updateprobleme bei der Kreuzung von Rechtsleben und säkulärem Staat finden sich auch bei der Software.

Da nehmen die Helden der langen Dateinamen eine gründliche Zugriffskontrolle vor, wenn man eine Datei auf einem Webserver haben will. Das ist im Handbuch von Microsoft nett und korrekt dokumentiert. Man kann es nicht nur glauben, sondern es funktioniert sogar. Wenn man jedoch den Namen des Herrn der Daten statt „Mahlzeitenabrechnung_Priesterseminar“ mit „Mahlzeit“ ansprach im alttestamentarischen 8+3 Format, bekam man alles ohne Zugangskontrolle; eine Art Daten-Abendmahl Online (Disclaimer für den Vertrieb der Zeitschrift in Bayern: das Pluszeichen ist kein Kreuz im Sinne eines religiösen Bekenntnisses). Diese 8+3 Bit-Mahlzeit Online hat längst ein Bugfix. Doch bei so mancher Herrschaftsbewahranstalt wird ein Bugfix am Bug fixiert statt implementiert und ist noch nach Erscheinen dieser Zeitschrift wirksam. Ob Gläubige das nicht merken, weil sie in deutschen Kirche als Einstiegsdroge Nebelschwaden und Alkohol im Gottesdienst bekommen, kann dahingestellt bleiben.

Als Tatsache kann jedoch festgestellt bleiben, daß zumindest Opfer das Recht auf deftige Darstellung eines Glaubensbekenntnisses haben. Bis ins wievielte Glied das für die verhinderten Kinder der ermordeten Hexen gilt, kann dahingestellt bleiben. Viele Hexen waren weise Frauen und deren Kinder wären bestimmt keine plattweltgläubigen Deppen geworden. Ich nutze seit Jahren die Schreibweise Häckse als weibliche Form. Wer etwas wissen möchte über die unterschiedlichen Rollen der Teufel in der Geschichte, der lese die Seite

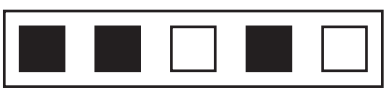
http://www.lucifer.de/texte/geschichte.htm

Auch das ist eine URL, die man sich merken kann mit der Standard-Methode URL-Raten.

Das als URL-Name ist Weisheit im Detail, jenseits von 8+3. Wer über die Rolle der Bits und der Datennetze, Häcksen und den Einfluß von Licht und Erleuchtung sowie das Verbot des freien Blicks durch Schleier, Nebel und Opium nachdenkt, tut mehr für Freiheit und Frieden als derjenige, der bloß ein T-Shirt mit Schwein am Kreuz trägt oder eine Web-Seite kopiert, weil er „dagegen“ ist, daß Fundamentalisten die Welt nicht begreifen.

Diese Ruhe gilt es zu lernen.

wau@ccc.de



From: spaf@cs.purdue.edu

- ein Stück (Use-)Net(z)geschichte

Gene Spafford war der Vorgänger von Tale (David Lawrence). Diesen Artikel schrieb er kurz vor seiner Amtsübergabe an Tale und seinem eigenen Rückzug aus dem Usenet.

(Dank für die Weiterleitungen an Hinrich Schramm und Gert Döring)

Date: 29 Apr 1993 19:01:12 -0500

There is a Zen adage about how anything one cannot bear to give up is not owned, but is in fact the owner. What follows relates how I am owned by one less thing....

About a dozen years ago, when I was still a grad student at Georgia Tech, we got our first Usenet connection (to allegra, then being run by Peter Honeyman, I believe). I'd been using a few dial-in BBS systems for a while, so it wasn't a huge transition for me. I quickly got „hooked": I can claim to be someone who once read every newsgroup on Usenet for weeks at a time!

After several months, I realized that it was difficult for a newcomer to tell what newsgroups were available and what they covered. I made a pass at putting together some information, combined it with a similar list compiled by another netter, and began posting it for others to use. Eventually, the list was joined by other documents describing net history and information.

In April of 1982 (I believe it was — I saved no record of the year, but I know it was April), I began posting those lists regularly, sometimes weekly, sometimes monthly; the longest break was for 4 months a few years ago when I was recovering from pneumonia and poor personal time management. (Tellingly, only a few people noticed the lack of postings, and almost all the mail was „When will they come out?" rather than „Did something happen?") As time went on, people began to attach far more significance to the posts than I really intended. It was flattering for a very short time, and a burden for most of the rest; there is no telling how much time I have devoted over the last decade to answering questions, editing the postings, and debating the role of newsgroup naming, to cite a few topics. I really tired of being a „semi-definitive" voice.

Starting several years ago, at about the time people started pushing for group names designed to offend or annoy others, or with a lack of concern about the possible effects it might have on the net as a whole (e.g., rec.drugs and comp.protocols.tcp-ip.eniac) I began to question why I was doing the postings. I have had a growing sense of futility: people on the net can't possibly find the postings useful, because most of the advice in them is completely ignored. People don't seem to think before posting, they are purposely rude, they blatantly violate copyrights, they crosspost everywhere, use 20 line signature files, and do basically every other thing the postings (and common sense and common courtesy) advise not to. Regularly, there are postings of questions that can be answered by the newusers articles, clearly indicating that they aren't being read. „Sendsys" bombs and forgeries abound. People rail about their „rights" without understanding that every right carries responsibilities that need to be observed too, not least of which is to respect others' rights as you would have them respect your own. Reason, etiquette, accountability, and compromise are strangers in far too many newsgroups these days.

I have finally concluded that my view of how things should be is too far out-of-step with the users of the Usenet, and that my efforts are not valued by enough people for me to invest any more of my energy in the process. I am tired of the effort involved, and the meager — nay,

Subject: That's all, folks

nonexistent — return on my volunteer efforts.

This hasn't happened all at once, but it has happened. Rather than bemoan it, I am acting on it: the set of „periodic postings" posted earlier this week was my last. After 11 years, I'm hanging it up. David Lawrence and Mark Moraes have generously (naively?) agreed to take over the postings, for whatever good they may still do. David will do the checkgroups, and lists of newsgroups and moderators (news.lists), and Mark will handle the other informational postings (news.announce.newusers).

I'm not predicting the death of the Usenet — it will continue without me, with nary a hiccup, and six months from now most users will have forgotten that I did the postings...those few who even know now, that is. That is as it should be, I suspect. Nor am I leaving the Usenet entirely. There are still a half-dozen groups that I read sometimes (a few moderated and comp.* groups), and I will continue to read them. That's about it, though. I've gone from reading all the groups to reading less than ten. Funny, though, the total volume of what I read has stayed almost constant over the years. :-)

My sincere thanks to everyone who has ever said a „thank you" or contributed a suggestion for the postings. You few kept me going at this longer than most sane people would consider wise. Please lend your support to Mark and David if you believe their efforts are valuable. Eventually they too will burn out, just as the Usenet has consumed nearly everyone who has made significant contributions to its history, but you can help make their burden seem worthwhile in between.

In closing, I'd like to repost my 3 axioms of Usenet. I originally posted these in 1987 and 1988. In my opinion as a semi-pro curmudgeon, I think they've aged well:

Axiom #1: „The Usenet is not the real world. The Usenet usually does not even resemble the real world."

Corollary #1: „Attempts to change the real world by altering the structure of the Usenet is an attempt to work sympathetic magic — electronic voodoo."

Corollary #2: „Arguing about the significance of newsgroup names and their relation to the way people really think is equivalent to arguingwhether it is better to read tea leaves or chicken entrails to divine the future."

Axiom #2: „Ability to type on a computer terminal is no guarantee of sanity, intelligence, or common sense."

Corollary #3: „An infinite number of monkeys at an infinite number of keyboards could produce something like Usenet."

Corollary #4: „They could do a better job of it."

Axiom #3: „Sturgeon's Law (90% of everything is crap) applies to Usenet."

Corollary #5: „In an unmoderated newsgroup, no one can agree on what constitutes the 10%."

Corollary #6: „Nothing guarantees that the 10% isn't crap, too."

Which of course ties in to the recent: „Usenet is like a herd of performing elephants with diarrhea - massive, difficult to redirect, awe-inspiring, entertaining, and a source of mind-boggling amounts of excrement when you least expect it." —spaf (1992)

„Don't sweat it — it's not real life. It's only ones and zeroes."

— spaf (1988?)

Dorfrecht aktuell

In München wurde von der Wirkung her Felix Somm für sozial nützliches Wirken verurteilt. Richter Hubbert begriff sich als Bitmauerschützer ohne zu begreifen, daß er nichts begriffen hatte. Denn er glaubte an seine Sachkompetenz beim Internet. Das bewies die mündliche Urteilsbegründung. Das Urteil wird weniger Bestand haben als das Verbot des Papstes gegen die erste europäische Enzyklopädie von Diderot und dAlembert, einer Sammlung des Wissens. Damals wie heute: sozial nützliches verboten.

Dank Internet ist immer mehr Wissen der Welt nur ein paar Mausklicks entfernt. Als positive Vision ließ John F. Kennedy Wissen messen. Der Goldberg-Report fand 1963, für alle Bücher der USA Kongreßbibliothek zusammen bräuchte man grob 10 hoch 13 Bits. Heute gibt es für soviele Nullen ein Alltagswort. ComputerBILD erklärt das Terabyte und http://www.alexa.com versucht, viel vom Internet-Inhalt zu speichern. Als „alte Version“ des Netzes vor ein, zwei Jahren haben sie zwei Terabyte, derzeitiger Ausbau 8 TB. Das ist ein Datenhaufen, der acht mal so groß ist wie die Gesamtbibliothek des US-Kongresses. Und da kommt ein Amtsrichter und meint, er habe Internet begriffen und sei urteilsfähig. Er ist mental nicht mal auf dem Stand von 1993 mit damals weltweit vier - ich wiederhole: vier - WWW-Servern. Hinzu kommt die Verdoppelung des Datenverkehrs derzeit grob alle hundert Tage.

Im CCC wird über Weiterentwicklung diskutiert, über Petabytes. Uli Sieber lag viele Nullen darunter, als er den Stand von 1995 anschaulich darstellte. Der Richter fand es machbar, täglich zwanzigtausend Strafverfahrensakten auf problematische Inhalte durchzuflöhen. Der Staatsanwalt begriff, daß er sich vergaloppiert hat und plädierte auf Freispruch. Vergeblich.

Im Rückblick geht der Begriff „Index“ zurück auf die Liste der Bücher, die ein Christenmensch nicht lesen sollte. Nach der Leibeigenschaft blieb die geistige Knechtschaft mit „cujus regio, ejus religio“: der Fürst bestimmt, woran die Untertanen glauben und die Erde ist eine Scheibe. Dabei hatten bereits die alten Griechen eine Vorstellung von Planetenbahnen. Sie nutzten einfachste Hilfsmittel. Einer steckte einen Stock in den Boden, beobachtete Sonne und Schattenwurf, dachte sich etwas und schrieb es auf. Das gehört ins Internet als Weltkulturerbe. Viele Jahrhunderte später zwang der Papst Galileo zum Widerruf. Die Geschichte der Scheiterhaufen gehört auch zum Weltkulturerbe.

Doch nicht nur kirchliche Macht, auch weltliche war kulturblind. Im alten Rom wurde die Null verboten, aus Angst vor Rechenverbrechen. Denn Computerkriminalität gab es bereits auf dem römischen Marktplatz bei Wachstäfelchen mit Strichen drin. Ein bißchen ändern und schon stand da „zehn“ statt „fünf“. Einem ein X für ein U vormachen hieß das. Weil die klassischen Bedenkenträger noch weit schlimmere Verbrechen mit dem arabischen Zahlensystem befürchteten, wurde die Null verboten.

Das Verbot der Null war Behinderung einer sozialen Erfindung ähnlich dem Urteil gegen Somm. Statt Bildung zu fördern für die Suche nach den edelsten Bits im Netz, Ausbildung zum informationellen Trüffelschwein, werden Abermillionen investiert in Software vom Typ Dreckschwein mit dem Zweck, mehr Dreck schneller zu finden. Das kann nur schief gehen. Es wird zukünftigen Generationen eine Mahnung sein wie die platte Weltsicht von Nolte. TV Phoenix dokumentierte, daß die Kulturverbotsministerin Sex im Internet erst ab 23 Uhr erlauben wollte. Im CCC meinte einer, es sei schlimmer. Denn das habe sie auch im Ausschuß in Bonn vertreten und dort kam die Nachfrage „23 Uhr: welche Zeitzone“. Das hat sie nicht verstanden. Plattwelt kennt nur eine Zeit.

Von Bob Jungk habe ich gelernt: think positive. Zwar droht der Zensurstaat als Atomstaat des Informationszeitalters. Doch wir wissen, was wir dagegen setzen: das Weltkulturerbe auf jedem Schreibtisch, per Knopfdruck erreichbar. Das Internet ist das erste Universalmedium der

Weltkulturerbe auf jeden Schreibtisch jetzt.

Geschichte und jeder Mensch mit Netzzugang kann dort schreiben. Da müssen positive Inhalte rein. Kulturelle Bedenkenträger in Europa pennen. In den USA stehen jetzt, jetzt! die Maschinen, um die Bibliotheken ins Netz zu bringen. Bücher werden nicht mehr zerschnitten oder so: man legt den wertvollen Wälzer vorn in die Maschine, die macht aus dem Buch Bits und hinten kommt es unbeschädigt heraus.

Konservative Buchkonservatoren wurden von dieser Maschine überzeugt. Europa hat noch nicht begriffen, daß es sowas gibt. Das könnte sich ändern, wenn Jesuiten eigene e-Mail-Adresse und Webspace ab Zeitpunkt Befruchtung als Menschenrecht einsehen. Andere Regionen versorgen, deren Kultur einbringen. Full IP für alle. Glasfasern rings um Afrika. In Alexandria kommen dicke Glasfaserbündel aus der Erde. Die Wahl des Platzes war Signal. Einst zerstörten Kulturbanausen dort die wohl erste große Weltbibliothek. Wir müssen Freiheit der Kommunikation und Austausches von Wissen fördern und destruktive Kräfte genau beobachten. Das Internet ist nicht einmal im Krabbelalter. Derzeit zeigt sich ein historischer Bruch. Erst ab ca. 1995 ist „vieles“ drin und vorher „wenig“. Das zu ändern, ist Aufgabe der Kulturpolitik in Verbindung mit aufgeklärten Menschen. Das Weltkulturerbe im Internet erleichtert es, mit dunklen Seiten der Informationsgesellschaft - der modernen Version des „X für U“ - zurecht zu kommen.

Job ist, dies Kulturträgern klar zu machen. Genau dann kommen wir mit den ewigen Nörglern klar, die es seit Erfindung des Rades gab und weiter geben wird. Das Netz entwickelt ein Stück weit Eigenintelligenz. Erste Gedankenspuren bahnen sich zu Wegen. Derzeit schätze ich es ein im Bereich Qualle: man kann versuchen, das Internet ans Kreuz zu nageln vor Gericht als eine Art Opfer für eigenes Versagen, aber das Ding lebt einfach weiter. Es wächst weiter, wird schlauer und freier. Gute Inhalte beschleunigen das Positive. Wie einst bei Büchern.

Weil Thüringer Gelehrte Angst hatten vor zuviel Büchern durch verbesserte Drucktechnik, ging der Erfinder Koenig nach London. Die erste dampfbetriebene Druckmaschine war bei der TIMES. Soviel als „Standortargument“ des Mittelalters. Erfinder Koenig wollte mehr Kultur, bezahlt hat eine Zeitung. Bei ALDI gibt es Festplatten im GB-Bereich. Bei Verdoppelung der Hardwareleistung alle 18 Monate steht in 15 Jahren das TB im Supermarkt und jeder tendenziell eine Großbibliothek auf dem Schreibtisch. Beschleunigen ist Zielrichtung, Bündelung der konstruktiven Kräfte der Gesellschaft. Von Druck-Erlaubnis kam es zum Jedermannrecht auf Mediendienste. Wie anders soll man eine Homepage bei Geocities oder im Königreich Tonga nennen? Der Streit zwischen Bundes- und Landesrecht ist längst entschieden, gegen beide. Wir haben Weltrecht. Heute. Und Dorfstörungen.

Wer eine Homepage baut, braucht von Netztechnik ebensowenig zu verstehen wie vom Strom beim Druck auf einen Lichtschalter. Ich erlebte, wie ein Kind einen Lichtschalter begreift. Denn vor rund 20 Jahren montierte mein Nachbar einen Kinderlichtschalter ganz weit unten. Die Tochter begann gerade zu krabbeln. Sie brauchte rund einen halben Tag zum Begreifen ihres Lichtschalters. Die Montage mußte besonders sorgfältig sein, um Betriebsrisiken durch erfinderische Kleinkinder zu minimieren. Das gehört zu den elterlichen Aufgaben: wer einen Schalter zugänglich macht, trägt auch die Verantwortung. Bedenkenträger vom Typ „Messer, Gabel, Schere, Licht sind für kleine Kinder nicht“ hatten keine Verfügungsgewalt über die Wohnung. Sorgfalt ist heute Elternpflicht beim Umgang mit dem Internet. Auch dort gibt es rote und grüne Ampeln. An den Straßen werden die Kinder ja auch nicht in Käfigen gehalten, um Unfälle zu vermeiden, sondern auf die Risiken vorbereitet. Elternpflichten gelten im Datenverkehr wie im Straßenverkehr. Fortbildung in der Schule: Erstkläßler an die Suchmaschinen!

Wau Holland, wau@ccc.de

Hier wäre Platz für

deinen

Artikel gewesen.

mailto: ds@ccc.de

Bestellungen, Mitgliedsanträge und Adreßänderungen bitte senden an:

CCC e.V., Schwenckestr. 85, D-20255 Hamburg

Adreßänderungen auch per Mail an office@ccc.de

Der Mitgliedsfetzen

Mitgliedsanträge und Datenschleuderabonnement

o Satzung + Mitgliedsantrag
(DM 5,00 in Briefmarken)

o Datenschleuder-Abo
Normalpreis DM 60,00 für 8 Ausgaben

o Datenschleuder-Abo
Ermäßigter Preis DM 30,00 für 8 Ausgaben

o Datenschleuder-Abo
Gewerblicher Preis DM 100,00 für 8 Ausgaben
(Wir schicken eine Rechnung)

Die Kohle liegt

o als Verrechnungsscheck
o in Briefmarken

bei bzw.

o wurde überwiesen am ___.___._____ auf
Chaos Computer Club e.V., Konto 59 90 90-201
Postbank Hamburg, BLZ 200 100 20

Ort/Datum

_____

Unterschrift

_____

Name

_____

Straße

_____

PLZ, Ort

_____

Tel/Fax

_____

Der Bestellfetzen

Literatur

_____ DM 29,80 Deutsches PGP-Handbuch, 3. Auflage + CD-ROM

_____ DM 5,00 Doku zum Tod des „KGB“-Hackers Karl Koch

_____ DM 25,00 Congressdokumentation CCC ‘93

_____ DM 25,00 Congressdokumentation CCC ‘95

_____ DM 25,00 Congressdokumentation CCC ‘97

_____ DM 50,00 Lockpicking: Über das Öffnen von Schlössern

Alte Datenschleudern

_____ DM 50,00 Alle Datenschleudern der Jahre 1984-1989

_____ DM 15,00 Alle Datenschleudern des Jahres 1990

_____ DM 15,00 Alle Datenschleudern des Jahres 1991

_____ DM 15,00 Alle Datenschleudern des Jahres 1992

_____ DM 15,00 Alle Datenschleudern des Jahres 1993

_____ DM 15,00 Alle Datenschleudern des Jahres 1994

_____ DM 15,00 Alle Datenschleudern des Jahres 1995

_____ DM 15,00 Alle Datenschleudern des Jahres 1996

_____ DM 15,00 Alle Datenschleudern des Jahres 1997

Sonstiges

_____ DM 50,00 Blaue Töne / POCSAG-Decoder / PC-DES Verschlüsselung

_____ DM 5,00 1 Bogen „Chaos im Äther“

_____ DM 5,00 5 Aufkleber „Kabelsalat ist gesund“

+ DM 5,00 Portopauschale!

_____ Gesamtbetrag

Die Kohle liegt

o als Verrechnungsscheck (bevorzugt)
o in Briefmarken

bei bzw.

o wurde überwiesen am ___.___._____ auf
Chaos Computer Club e.V., Konto 59 90 90-201
Postbank Hamburg, BLZ 200 100 20

Name

_____