die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

»Bundestagspräsident Thierse wischte die Kritik bei der Präsentation der Kampagne am Donnerstag schnell vom Tisch. Deutschland sei kein Verfolgungsstaat, außerdem gebe es in der Gesellschaft keinen Widerstand gegen die Verfolgung von Straftätern durch Lauschangriffe, sagte er. Die Kritiker hätten die Kampagne wohl "falsch verstanden", so Thierse. Ihre Vorhaltungen seien, so der Mann mit dem zweithöchsten Amt im Staate wörtlich, "dummes Zeug".«

Quelle: spiegel-online, http://www.spiegel.de/politik/deutschland/0,1518,199611,00.html

Last-Minute-Korrekturen an einem Plakatmotiv aus der Bundestagskampagne "Entscheidungen für die Freiheit" – die es dann irgendwie doch nicht in die endgültige Version geschafft haben…

ISSN 0930-1054 • Erste Ausgabe 2002
EUR **2,50 bitteschön**
Postvertriebsstück C11301F

#77

Erfa-Kreise

Bielefeld	im Café Parlando, Wittekindstraße 42, jeden Dienstag (außer feiertags) ab 18h	*http://bielefeld.ccc.de/* *<mail@bielefeld.ccc.de>*
Berlin, CCCB e.V.	Marienstr. 11, Berlin-Mitte, *Briefpost: CCC Berlin / Postfach 640236 / D-10048 Berlin* Club Discordia jeden Donnerstag zwischen 17.00 und 23.00 Uhr in den Clubräumen. *Achtung: wir sind wieder in den alten – endlich renovierten – Räumen im Hinterhaus zu finden!*	*Fon: +49.30.285.986.00* *Fax: +49.30.285.986.56* *Aktuelles (ja, wirklich!) unter http://berlin.ccc.de/*
Düsseldorf, CCCD/ Chaosdorf e.V.	"zakk", Fichtenstr. 40 jeden 2. Dienstag im Monat ab 19.00 Uhr	*http://duesseldorf.ccc.de/*
Frankfurt am Main, cccffm	Club Voltaire, Kleine Hochstraße 5, donnerstags ab 19 Uhr	*http://www.ffm.ccc.de/*
Hamburg (die Dezentrale)	Lokstedter Weg 72 jeden Dienstag ab ca. 20.00 Uhr in den Clubräumen. Der jeweils erste Dienstag im Monat ist Chaos-Orga-Plenum (intern). An allen anderen Dienstagen ist jede(r) Interessierte herzlich willkommen. Termine aktuell unter *http://hamburg.ccc.de/bildungswerk/*	*http://hamburg.ccc.de/* *Fon: +49.40.401.801.0,* *Fax: +49.40.401.801.41,* *Voice: +49.40.401.801.31.*
Hannover, Leitstelle511	Kneipe "kleines Museum" in Linden, am Mittwoch der zweiten Woche des Monats ab 20h	*https://hannover.ccc.de/*
Karlsruhe, Entropia e.V.	Gewerbehof, Steinstraße 23, jeden Sonntag ab 19:30h	*http://www.entropia.de/*
Köln, Chaos Computer Club Cologne (C4) e.V.	Vogelsanger Str. 286, *50° 56' 45" N, 6° 51' 02" O (WGS84),* jeden letzten Donnerstag im Monat um 19:30h	*Fon: +49.221.546.3953* *<oeffentliche-anfragen@koeln.ccc.de>,* *http://koeln.ccc.de/*
München, muCCC	Blutenbergstr. 17, jeden zweiten und vierten Dienstag im Monat ab 19:30h	*http://www.muc.ccc.de/*
Ulm	Treffen Montags ab 19.30 Uhr entweder im 'Café Einstein' an der Uni Ulm oder beim Internet Ulm/Neu-Ulm e.v. (am Besten vorher per Mail anfragen!). Regelmäßige Vorträge im 'Chaos Seminar': http://www.ulm.ccc.de/chaos-seminar/	*http://ulm.ccc.de/* *<mail@ulm.ccc.de>*

Chaos-Treffs

Aus Platzgründen können wir die Details aller Chaos-Treffs hier nicht abdrucken. Es gibt aber in den folgenden Städten Chaos-Treffs mit Detailinformationen unter *http://www.ccc.de/regional/*: Bochum, Bremen, Darmstadt, Erlangen/ Nürnberg/Fürth, Freiburg i. Br., Gießen / Marburg, Trier, Kiel, Münster / Osnabrück, Saarbrücken, Stuttgart, Emden

Die Datenschleuder Nr. 77

Erste Ausgabe 2002

Herausgeber

(Abos, Adressen, Verwaltungstechnisches etc.)
Chaos Computer Club e.V. /Lokstedter Weg 72, D-20251 Hamburg, Fon: +49.40.401.801.0, Fax: +49.40.801.401.41, <office@ccc.de>

Redaktion

(Artikel, Leserbriefe, Inhaltliches, etc.)
Redaktion Datenschleuder, Postfach 640236, D-10048 Berlin, Fon: +49.30.285.986.56, <ds@ccc.de>

Druck

Pinguindruck, Berlin; http://pinguindruck.de

Layout, ViSdP und Mädchen für alles

Tom Lazar, <tom@tomster.org>

Redakteure dieser Ausgabe

Tom Lazar, Andy Müller-Maguhn und Tina Lorenz

Autoren dieser Ausgabe

Andy Müller-Maguhn, Erdgeist, Horst-Walter Schwager, Stefan Krecher, Tom Lazar, Sarah Spiekermann, Nika Bertram, Lars Weiler, Christine Ketzer, Ingo Schwitters und Tina Lorenz, Christopher Creutzig, Hubert Feyrer und Marius Strobl, Bastian Ballmann, Sebastian Zimmermann, R. Schrutzki.

Die Lizenz zum Denken

Intellectual Property, Digital Rights Management, End User Licence Agreement, Digital Millenium Copyright Act, Region Codes bei DVDs – das Ungeheuer hat viele Köpfe. Hinter all diesen (und noch vielen weiteren) Ansätzen steht der gemeinsame Grundgedanke der Restriktion. Was *per se* auch nicht verkehrt ist. Selbst freiheitliche Verfassungen wie z.B. die U.S.-amerikanische oder das deutsche Grundgesetz kommen ohne Verbote nicht aus. Aber immerhin beziehen sich einige davon (etwa Strafgesetzbuch oder Urheberrecht) nicht nur auf das Volk, sondern auch auf die Regierung (das Verbot von Zensur beispielsweise). Zudem gewähren sie andererseits auch *Rechte* (etwa auf Bildung, freie Meinungsäußerung, Wahlen, private Kopie usw.) Die Polarität liegt also zwischen Volk und Regierung und irgendwie scheint sich das mit den Restriktionen und Rechten die Waage zu halten. Bis jetzt, jedenfalls.

Mit der zunehmenden Digitalisierung der Gesellschaft wird dieses Gleichgewicht nämlich immer mehr entstellt. Zum einen verschiebt sich die Polarität weg von Staat und Bürger hin zu Industrie und Konsument. Und zum anderen geht der Trend klar weg von den Rechten des Einzelnen hin zu den Rechten der Industrie. Und der Staat macht (fast überall auf der Welt) brav mit.

Da *pro forma* ja noch das Deckmäntelchen des *opt-out* gilt (alles, was nicht explizit verboten ist, ist erlaubt) sehen sich Konsumenten und Bürger überall auf der Welt mit einer zunehmenden Lawine von Restriktionen konfrontiert – schön verpackt in *Licence Agreements*, zusammen mit den passenden Gesetzen, die das Umgehen dieser Restriktionen unter teilweise drakonische Strafen stellen.

Weshalb dieser besorgniserregende Trend mit der Digitalisierung unseres Alltages zu tun hat, dürfte klar sein: viele Vorgänge und Beschränkungen der "realen" Welt haben in der "virtuellen" kein vernünftiges Pendant oder sind schlichtweg nicht vorhanden. Dass beispielsweise nationale Grenzen und Jurisdiktionen im Internet sinnfrei werden oder dass die technische Möglichkeit von unbeschränkter Vervielfältigung bzw. die völlige Entkoppelung "geistigen Eigentums" von dessen Trägermedium eine radikal neue Situation schaffen, leuchtet ein.

Was vielen aber überhaupt nicht einleuchtet steht im Kontext der Frage, wer oder was sich den neuen Zeiten nun anpassen soll: in der ganzen Diskussion scheint implizit vorausgesetzt, dass die Industrie geradezu das *Recht* habe, an ihren alten Vertriebsmechanismen und Handelsmodellen festzuhalten – dass und Gesetzgeber und Konsument sich gefälligst anzupassen haben. Diese Arroganz wird dadurch noch verschärft, dass ihrer Durchsetzung reihenweise Grundrechte zum Opfer fallen: Recht auf freie Meinungsäußerung, Freiheit der Lehre, Verbot von Zensur, um nur einige zu nennen.

SAP und „Sicherheit"

Ich besuchte vor einiger Zeit an einem Samstag, das genaue Datum ist mir leider entfallen, den Tag der offenen Tür bei SAP in Walldorf, Baden, dem (selbsternannt) weltweit führenden Anbieter von "E-Business-Softwarelösungen".

Dort wurden auch einige (ca. 20) Windows NT-Workstations für die Besucher zur Verfügung gestellt. Diese waren an das Internet und das LAN zumindest dieses Gebäudes angeschlossen. Der Internetzugang war uneingeschränkt, das LAN nur teilweise nutzbar. Es gab einen sogenannten „Marktplatz", ein Netzlaufwerk auf das alle Benutzerkonten Lese- und Schreibzugriff besaßen. Jedoch konnte der Zugriff auf sämtliche Netzlaufwerke recht einfach erlangt werden.

Wie schon einige Zeit bekannt besteht bei dem Betriebssystem Windows NT die Möglichkeit, den Anmeldebildschirmschoner logon.scr in C:\WINNT\SYSTEM32\ mit der „Eingabeaufforderung" cmd.exe, welche im selben Verzeichnis zu finden ist, zu überschreiben (im Prinzip könnte man auch die cmd.exe in logon.scr umbenennen, eigentlich ist das sogar einfacher) und somit mindestens die Rechte eines lokalen Administrators zu erlangen. Das ist möglich, weil NT den Anmeldebildschirmschoner standardmäßig nach 15 Minuten startet. Ist dieser aber die cmd.exe unter falschem Namen, nämlich logon.scr, so wird diese anstelle des Bildschirmschoners ausgeführt, und es steht somit eine DOSbox zur Verfügung.

Aus dieser heraus lassen sich sämtliche ausführbaren Dateien, unter anderem auch der Windows Explorer, starten. Der Windows Explorer dient zu Navigation auf den Festplatten und Netzlaufwerken des Systems und ist, wie die Verzeichnisstruktur selbst, baumartig angelegt. Diese Methode muss angewandt werden, da das Ausführen der cmd und somit des Explorers hierbei noch vor der Anmeldung geschieht, also Standartrechte der lokalen Administratorengruppe vergeben sind. Diese sind immer höher als Gast- bzw. normale Userrechte, oft darüber hinaus mit den Rechten eines Domänenadministrators zu vergleichen.

Spezialfall „SAP": Hier gestaltete sich die Prozedur leider nicht so einfach, da auf SYSTEM32 kein Zugriff auf Windowsebene möglich, und somit die cmd nicht zu erreichen war. Es gibt zwar noch die Möglichkeit die cmd auszuführen, indem man eine Batchdatei (Stapelverabeitungsdatei im Klartext mit Endung .bat) mit dem Inhalt „cmd" schreibt und diese dann ausführt, jedoch stand mir kein Editor zur Verfügung.

Das Problem konnte ich lösen, indem ich mir selbst von meiner Mailbox eine E-Mail mit der cmd im Anhang schickte, und eben selbige in einem mir zugänglichen Verzeichnis speicherte und von dort aus öffnete. Nun hatte ich die Möglichkeit oben beschriebenes Prozedere durchzuführen. Nach besagten 15 Minuten

---

Solange aber diese Prämisse unantastbar bleibt, werden es unsere einst verbrieften Grundrechte aus der "realen" Welt nicht in die "virtuelle hinüberschaffen". Und nicht nur das: wenn der Trend anhält, werden wir eines Tages in der "realen" Welt aufwachen und feststellen, dass wir sie auch dort verloren haben. (Einige Kopierschutzinitiativen schreiben z.B. *digitale* Inhaltsspeicherung *vor* – damit der Schutz auch greifen kann. Eine private VHS-Kopie einer DVD ist in diesem Szenario streng verboten, sogar dann, wenn ein Lehrer sie im Unterricht einsetzen will – seine Schule müßte erst eine entsprechende Lizenz erwerben.)

Und wenn dann aus dem bewährten *opt-out* via Heerscharen restriktiver *Licence Agreements* ein faktisches *opt-in* geworden ist (alles, was nicht explizit erlaubt ist, ist auf einmal verboten) wird uns das Lachen über eine "Lizenz zum Denken" im Hals stecken bleiben – nur, dass es dann zu spät für Gegenmaßnahmen ist.

Eine von vielen Möglichkeiten, die wir haben, ist die Angelegenheit auf breiter Front zu thematisieren. Die Industrie hofft auf die Gleichgültigkeit und Unwissenheit der Konsumenten (s. auch den Artikel "Happy Volksverarschung" auf S. 14). Wollen wir ihr diesen Gefallen wirklich tun?

In diesem Sinne: *Spread the Word!* <Tom Lazar>

Inhaltsverzeichnis

standen mir also alle Netzlaufwerke offen, wobei ich sagen muss dass ich nicht weiß ob es wirklich alle waren. Um das herauszufinden gibt es eine Methode, die ich in diesem Fall jedoch nicht angewandt habe.

Noch etwas Grundlegendes: Windows stellt mit Winfile, bei Win 3.x unter dem Namen Datei-Manager vertreten und bekannt, ein ähnliches Werkzeug wie den Explorer bereit. Der Unterschied ist die sehr bequeme und meines Wissens nach nicht abzustellende Funktion Ordner und Festplatten auf entfernten Rechnern als Netzlaufwerk zu verbinden und somit Zugriff zu erlangen. Zwar können auch diese Laufwerke gesperrt werden, jedoch wird das von vielen nachlässigen Administratoren außer acht gelassen.

Doch selbst wenn man seinen Zugriff auf diese Weise nicht ausbauen kann, so ist es doch möglich, sich einen sehr schönen Überblick über das gesamte verfügbare Netz zu verschaffen.

Das Ende vom Lied: Etwas erstaunt über die gebotenen Möglichkeiten eilte ich zum verantwortlichen Mitarbeiter der SAP der mir freundlich aber bestimmt zu verstehen gab dass ihn derartiges nicht interessiere. Schade. *Alexander Ehmann <erdbaerehmann@web.de>*

Sicherheit, Verschlüsselung und Passwörter

Wie kann ich mein (sic!) Festplatte allgemein mit einem Passwort versehen (nicht nur im Netzwerk). So dass ich immer ein Passwort eingeben muss um auf z.B. `E:` *zuzugreifen? Florian Bollhorst*

Entweder setzt Du ein Betriebssystem mit Sicherheitssystem ein, dann kannst Du während dem laufenden Betrieb das durch Konfiguration des Sicherheitssystems erreichen.

Oder aber Du meinst, dass man ohne Kennwort grundsätzlich nicht an die Daten kommen darf; dann solltest Du eine Software zum Verschlüsseln der Daten auf der Festplatte einsetzen.

Vorsicht: dadurch erreichst Du zwar, dass jemand wirklich das Kennwort braucht, wenn er nur Deine Festplatte hat. Dadurch erreichst Du aber noch keine "Sicherheit". Sicherheit und Verschlüsselung sind zwei völlig verschiedene Dinge.

Zunächst einmal solltest Du Dein Kennwort geeignet wählen – und das ist gar nicht so einfach. Du solltest nämlich am Besten ein längeres Kennwort als 8 Zeichen nehmen, das kräftig verwürfelt ist und nicht an irgendein Wort, ein Datum oder sonst was aus Deinem täglichen Leben oder aus irgendeiner Sprache oder Kultur erinnert.

Dann solltest Du zum Verschlüsseln eine Software nehmen, die ein sog. "hartes" Kryptographieverfahren verwendet, wie z.B. den neuen Kryptostandard AES.

Dann musst Du Deiner Software soweit Vertrauen schenken (können), dass sie keine Hintertür in die Verschlüsselung einbaut und auch wirklich geeignet arbeitet. Software von amerikanischen Herstellern muss beispielsweise eine Hintertür für den amerikanischen Auslandsspionage- Geheimdienst NSA haben, das ist Gesetz in den USA.

Ausserdem musst Du der Software soweit vertrauen, dass sie geeignet arbeitet, und nicht so dämlich, wie beispielsweise die Dateiverschlüsselung in Windows 2000, die zum Arbeiten unverschlüsselte Kopien Deiner zu schützenden Daten anlegt, und diese nur unzureichend wieder löscht, so dass man sie wiederherstellen kann.

Also schenkst Du natürlich insbesondere dem Hersteller der Software Dein Vertrauen, und ganz besonders seinen Programmierern. Du solltest Dir also überlegen, wem Du dieses Vertrauen entgegenbringst.

Dann musst Du Deinem Rechnersystem vertrauen können, auf dem Du die Festplatte verschlüsselst oder entschlüsselst, dass da keine Software läuft, die Dein Passwort oder Deinen Schlüssel mitliest und verrät, oder aber dass da keine Software läuft, die Deine Daten ausspäht, während Du selber den Schlüssel und/oder das Kennwort nutzt und somit die Daten zugänglich machst.

Das bedeutet insbesondere, dass derjenige, der Dein Rechnersystem verwaltet, wissen muss, was er tut, und nicht nur bei der Wahl der Hard- und Software Sicherheitsaspekte betrachtet hat, sondern auch bei der Konfiguration und Pflege des Systems entsprechend sorgfältig vorgeht. Wenn Dein Betriebssystem gar kein Sicherheitssystem hat, dann ist das ein grosses Problem, schliesslich ist es so gut wie unmöglich, so ein einigermassen sicheres System zu bekommen.

Ich höre aus Deiner Frage mal raus, dass Du Windows oder OS/2 einsetzt. Wenn es ein Windows NT basierendes System, also Windows NT, Windows 2000 oder Windows XP ist, dann hat Dein System ein Sicherheitssystem. Wenn es OS/2 ist, dann ist es möglich, dass Du ein Sicherheitssystem für das Dateisystem hast, es kann aber auch sein, dass nicht. Wenn Du Windows 95, Windows 98 oder Windows ME einsetzt, dann hat Dein System kein Sicherheitssystem. Damit erreichst Du sicher keine nennenswerte Sicherheit.

Es gibt viele Leute, besonders hier im Club, die Software von Microsoft soweit misstrauen, dass sie die Begriffe "Sicherheit" und "Microsoft" grundsätzlich nicht in einen Zusammenhang bringen wollen. So extrem sehe ich das nicht, aber schon sehr kritisch.

Gib mal "Verschlüsselung Windows Festplatte" oder "Verschlüsselung OS/2 Festplatte" in eine Suchmaschine Deiner Wahl ein, wenn Du nicht weisst, wo man Software bekommen kann, die die Daten auf einer Festplatte verschlüsselt. Falls Du das willst. Falls Du das so bewertest, dass Dir das Sicherheit bringt. *V.B*

Verfügbarkeit von PGP zunehmend eingeschränkt

Die Firma Networks Associates (NAI), vor kurzem noch Herausgeber der Verschlüsselungssoftware PGP, hat offenbar ihre geschäftlichen Aktivitäten im Bezug auf PGP verändert.

Verkündete NAI gerade mal einen Monat nach dem 11.09.2001, dass man PGP aus wirtschaftlichen Gründen nicht weiterentwickeln und die PGP-Produktpalette weitgehendst an ein anderes Unternehmen (das man noch suchen würde) zu veräußern wollen würde [1], so geht NAI nunmehr dazu über, sogar Betreiber von Seiten abzumehnen, die ältere Versionen von PGP zum download anbieten [2].

Welchen Zusammenhang das von der amerikanischen Regierung nach dem 11.09. gestartete Project "Operation Shield America" [3], die neuen Regelungen im Bezug auf den Verkauf und den Export von Kryptoprodukten dabei spielen, konnte im Detail noch nicht geklärt werden.

Nicht-europäische Quellen aus der Wirtschaft berichten schon länger, dass sie nicht verstehen, warum man bei NAI zwar PGP bestellen kann, dieses aber nicht geliefert wird. Immerhin erklären sich so wenigtens die "wirtschaftlichen" Gründe die NAI für die nicht-weiterentwicklung von PGP nennt.

[1] *http://www.heise.de/newsticker/data/anw-12.10.01-000/*

[2] *http://crypto.radiusnet.net/archive/pgp/index.html*

[3] *http://www.customs.gov/hot-new/pressrel/2001/1210-01.htm*

Zeig mir, was Du überträgst

Modems, Router, Krypto-Boxen – es gibt viele Geräte, die sensitive Daten übertragen. Die meisten davon haben irgendeine Form von Status-Anzeige, meistens mit mehr oder weniger blinkenden LEDs. Aber die zeigen ja bekanntlich nichts Sicherheitsrelevantes an, sondern nur, dass eine Verbindung besteht oder dergleichen, richtig?

Falsch. Wie Joe Loughry von Lockheed Martin und David A. Umphress von der Auburn University zeigen konnten, arbeiten auch LEDs, die nicht an einem Glasfaserkabel hängen, oftmals als Übermittler von Daten, mit einer erstaunlich guten Datenrate: Sie konnten bei 14 der 39 getesteten Geräte in bis zu 5 Metern Entfernung noch die übermittelten Daten abgreifen, und das bei Datenraten bis zu 56KBit/s. Fehlerfrei, versteht sich. Der technische Aufwand beschränkt sich auf ein Teleskop, einen schnellen Sensor und etwas Standardelektronik und das sendende Gerät hat absolut keine Chance, die Abhörmaßnahme festzustellen. Im Gegensatz zu "klassischen Strumangriffen" (tempest attacks) funktioniert diese Analyse natürlich nicht durch Wände hindurch, aber eine Fensterscheibe stellt noch kein Hindernis dar.

Nebenbei bemerkt verweisen die Autoren darauf, dass ein teilweise veröffentlichtes Paper der NSA Hinweise darauf enthält, dass LED-Anzeigen verräterisch sein könnten. Wie viel Geheimdienste davon schon wussten und eventuell schon Gebrauch davon gemacht haben, bleibt naturgemäß unklar.

Link: *http://applied-math.org/optical_tempest.pdf*

Eine weitere neu entdeckte optische Abhörmöglichkeit hat Markus Kuhn veröffentlicht: Röhrenmonitore bauen bekanntlich ihr Bild Pixel für Pixel auf, schnell genug hintereinander. Wie er nun experimentell zeigen konnte, genügt es keineswegs, dass der Monitor einem Angreifer "den Rücken zudreht", sondern mit einem schnellen Fotosensor ist es tatsächlich möglich, einen Monitor in einem dunklen Raum dadurch abzulesen, dass man das Flimmern auf der gegenüberliegenden Wand aufnimmt. Bei LCD-Schirmen funktioniert das technisch bedingt nicht, womit sie auch gegen diesen Abhörangriff wesentlich weniger anfällig sind. In sicherheitsrelevanten Bereichen sollten ohnehin CRT-Monitore durch LCD-Monitore ersetzt werden, da deren elektromagnetische Abstrahlung wesentlich geringer ausfällt.

Link: *http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf*

Zusammenfassung: *Christopher Creutzig, ccr@foebud.org*

Rupert Murdoch / NDS vs. Canalplus

Nutzung von Hackermethoden als Mittel, der Konkurrenz zu schaden.

Die ehemalige israelische Firma NDS [1], mittlerweile formell im britischen Besitz des *Rupert Murdoch*, hat nach Angaben eines Dienstleisters offensichtlich wissentlich und offensiv Hacker und Hackermethoden dazu genutzt, die Systeme des im PayTV-Bereich konkurrierenden Unternehmens Canal Plus zu schaden.

Oliver *Koemmerling*, Inhaber der Firma ADSR [2] und in der Szene auch als technischer Kooperationspartnerin Sachen Chipkartenuntersuchungen des unter unklaren Umständen verstorbenen Boris F. (alias *Tron*) bekannt ist dabei der Kronzeuge von Canal Plus. In seiner schriftlich niedergelegten Aussage [3] für Canal Plus vor einem kalifornischen Gericht bekennt er nicht nur, in Sachen "consultancy services in the field of microelectronics and software security" sondern auch bereits seit 1996 eng mit NDS operational security kooperiert zu haben "helping to defeat piracy" .

Nicht nur, dass Tron von dieser engen Zusammenarbeit zwischen Koemmerling und NDS Security nichts gewusst haben dürfte, auch eine etwas genauere Betrachtung der von Koemmerling mit "NDS operational security" bezeichneten Personen lässt einem die Haare zu Berge stehen. Handelt es sich hier in Europa um den maßgeblichen bei der Anwerbung von Tron in Erscheinung getretenen ehemaligen Scotland-Yard Mitarbeiter und dortigen Leiter einer Intelligence Abteilung, *Ray Adams*, der nach bisher nicht nachrecherchierbaren Gerüchten auch beteiligt an

einem britischen Unternehmen ehemaliger *Gladio* [4] Mitarbeiter ist.

In einem illustren Artikel aus dem Heimatland von Rupert *Murdoch* weist die Australian Financial Review [5] auch darauf hin, dass beispielsweise der Mitarbeiter aus dem Bereich, den *Kömmerling* "NDS operational security" nennt, in den USA ein "army counter-intelligence officer who had run sting operations in North America" sei.

Die Berliner Staatsanwaltschaft, die nachwievor Untersuchungen im Falle des verstorbenen Boris F. alias *Tron* verweigert, um herauszufinden, ob sich etwa Fingerabdrücke von Tron überhaupt am Gürtel befinden, der ihm um den Hals hing, zeigte sich von den neuen Erkenntnissen durch die auch im Fall Tron auftauchenden Zeugen Kömmerling unbeeindruckt. Auch die Tatsache, dass es mittlerweile als nachgewiesen gelten kann, dass der Gürtel um den Hals von Tron, an dem dieser aufgehängt aufgefunden wurde, überhaupt nicht sein Gürtel war [6], interessiert die Staatsanwaltschaft nicht weiter. Zitat [7]: "Dass die Möglichkeit besteht, auch mit einem ´fremden´ Gürtel Selbstmord zu begehen, liegt auf der Hand".

Welchen Zusammenhang das hier zu beobachtende annährend vorbildliche Verhalten der Berliner Justiz mit dem ehemaligen Arbeitsbereich von Herrn *Adams* zu tun hat, ist dabei nur die eine Frage. Zum anderen sollte der werte Leser noch wissen, dass der hier agierende Staatsanwalt *Bauer* im wesentlichen auf Anordnung des Oberstaatsanwalt *Wiedenberg* agiert. Dieser ist auch dafür zuständig gewesen, den mit einem Henkersknoten erhängt aufgefundenen ehemaligen Mitarbeiter der im Beliner Bankenskandal maßgeblichen Firma *Aubis* als Selbstmord zu deklarieren.

Wer eigentlich gegen einen Oberstaatsanwalt ermitteln kann und auch willig ist, dies zu tun, konnte noch nicht herausgefunden werden.

[1] News Data Services

[2] ADSR: *http://www.adsr.de/*

[3] Prozessunterlagen unter *http://www.actiononecanalplus.com/*

[4] GLADIO ist nur eine von mehreren Begriffen für die im Zeitalter des kalten Krieges von der NATO betriebenen sogenannten stay-behind-organisationen [SBO] der Nato. Hierzu gibt ist umfangreiche Literatur, auch im Netz erhältlich: *http://www.contramotion.com/sources/org/sbo* oder Suchmaschinen nach Wahl

[5] *http://afr.com/premium/commentopinion/2002/04/15/FFXDVLLSZZC.html*

[6] *http://www.ccc.de/~andy/CCC/Tron/20020307/*

[7] *http://www.ccc.de/~andy/CCC/Tron/20020508/*

[8] *http://www.contramotion.com/updates/persons/larsoliverp*

Crypto - SMS ?

In Berlin gibt es jetzt eine Bürgerinitiative für Sicherheit im Versand von Kurznachrichten. Diese berichtet abenteuerliches von einem SMS-Catcher und fragt, wie es mit Verschlüsselungsoptionen für SMS aussieht. Eine Gute Frage.

Im Netz: *http://www.bsvk.de/*

US-Wissenschaftler mißbrauchen Ratten als ferngesteuerte Spione

Die Deutsche Presseagentur (DPA) berichtete am 01.05.2002 im Bereich Wissenschaft über einen Bericht eines wissenschaftlichen Teams in der britischer Zeitschrift Nature (Bd. 417, S. 37). Die Wissenchaftler gaben an, mittels ins Gehirn implantierter Elektroden Ratten noch aus 500 Meter Entfernung zielgerichtet lenken zu können.

Sanjiv Talwar von der State University New York und seine Mitarbeiter schnallten den Ratten dabei entsprechende Ansteuerelektronik auf den Rücken, über den sie per Fernbedienung implantierte Elektroden im Gehirn ansprechen konnten. Mit entsprechend dosierten Stromschlägen reizten sie die Regionen, die normalerweise Signale von den Tasthaaren der Schnauze verarbeiteten und simulierten so Berührung entweder der rechten oder der linken Tasthaare. Bei entsprechend gewünschter Lenkungsänderung wurden zusätzlich Funktionen im "Belohnungszentrum" des Gehirns aktiviert.

Verbleibt die Frage, wie wir in Zukunft ferngesteuerte Congressbesucher erkennen...

Flugverbot nach dem 11.09. sorgte für wärmere Tage

Wenn auch nicht alle Bewohner Amerikas gleichermaßen in den Genuss der wärmeren Tage nach dem 11.09. kommen konnten, so halten Wissenschaftler einen Zusammenhang zwischen dem dreitägigen Flugverbot nach dem 11.09. und den daraufhin einsetzenden wämeren Tagen und kälteren Nächten für erwiesen.

Die am Himmel fehlenden Kondensstreifen, da jeglicher zivile Flugverkehr über den USA verboten war, sind als Ursache identifiziert. Das berichtet der amerikanische Meteorologe David J. Travis diese Woche auf einem Kongress der Amerikanischen Meteorologischen Gesellschaft in Portland.

Im Netz: *http://www.wissenschaft.de/sixcms/detail.php?id=122530*

Eine ganz reale Protest-Aktion

Von Tina Lorenz und Ingo Schwitters

Die Demonstration am 6. April 2002 gegen die von der Bezirksregierung Düsseldorf angeordneten Zensurmassnahmen im Internet war ein grosser Erfolg und hat mehrere Dinge gezeigt, unter anderem, dass Nerds nicht nur virtuell existieren. Ein Bericht vom ersten Aufmarsch der Computer Freaks dieser Art.

Die Pressekonferenz vor der Demo sah noch ganz gemütlich aus: eine Handvoll Vertreter der schreibenden Zunft sass mit Alvar, dem Initiator von *odem*, Ingo, dem Organisator der Demo, und Andy, seines Zeichens Pressebespasser, um einen Tisch herum, und liess sich erklären, warum diese Demonstration wichtig sein würde, für alle Bürger NRWs und bundesweit.

Danach Szenenwechsel: Auf dem Platz, auf dem die Demonstration starten sollte, standen zwei mittelgrosse Fahrzeuge und ein paar versprengte Nerds, die nervös mit Plakaten und ähnlichem hantierten. Na heiter, eine Demonstration mit sage und schreibe zwölf Leuten! Die für unseren Schutz abgetellten grünen Männchen waren noch deutlich in der Überzahl, als plötzlich von allen Seiten her Leute auftauchten. Der ganze Platz hatte sich unmerklich mit Menschen gefüllt, die die phantasievollsten Plakate mitgebracht hatten. 'Hoch die internationale Connectivität', 'Zensur ist immer falsch!' und 'Wir sind dagegen' konnte man unter anderem auf den Schildern lesen. Das Wetter war prima, der Veranstalter reichlich hibbelig, alles im Rahmen der normalen Parameter also. Der Zug durch die Düsseldorfer Innenstadt konnte beginnen.


Zensur zum Anfassen: wer die Massen mobilisieren will muss plastisch arbeiten...

Auf dem einen Wagen hatten sich Nerds versammelt, die mit zugeklebtem Mund und zugehaltene Augen ihre eingeschränkte Meinungs- und Informationsfreiheit darstellten: *Aufklärung statt Filtern* stand auf den Schildern neben ihnen. Der andere Wagen sorgte für freundliche Musik, immer wieder unterbrochen von Parolen und Schlagwörtern zur Erbauung der Demonstranten. Man verstand nicht viel, stimmte aber in das allgemeine Gejohle mit ein.

Dann: Zwischenkundgebung mit Blick auf den Rhein. Es wurden jede Menge Flyer an die staundende Menge verteilt, die wissen wollte, was los ist. Es sprach unter anderem padeluun aus Bielefeld, der mit Mühe auf den Verkündungswagen geklettert war. Durch seine Skates und mit dem Megaphon war er eher das mobile Einsatzkommando unserer Demo. Scharf wurde Herr Büssow, der Regierungspräsident von Düsseldorf, in Ansprachen attackiert.

Dann ging es weiter, die eigens für uns abgesperrten Strassen hinunter zum Gebäude der Bezirksregierung Düsseldorf. Dort angekommen, bauten wir uns mit den grossen Transparenten vor dem Eingang der Bezirksregierung auf. Erwartungsgemäss kam ein beleibter Mensch heraus, Herr Riesenbeck, der Vertreter von Büssow. Erstaunlicherweise trat dann aber ein Mann aus dem Schlagschatten des anderen, mit dem wir nicht unbedingt gerechnet hatten: es war Büssow selbst, der unbestätigten Gerüchten nach extra seinen Urlaub unterbrochen hatte, um sich der protestierenden Masse zu stellen.

Was war passiert?

Bereits am 8.Februar 2002 hat die Bezirksregierung Düsseldorf Sperrungsverfügungen gegen mehr als 80 Anbieter von Internet-Zugängen erlassen. Provider werden darin aufgefordert, bestimmte Webseiten nicht mehr zum Kunden durchzustellen. Die Bezirksregierung beruft sich dabei auf ihre Kompetenz als Landes-Auf-

sichtsbehörde für den gesetzlichen Jugendschutz und die "Ahndung von Ordnungswidrigkeiten" gem des Mediendienstestaatsvertrags. Ein sauberes deutsches Internet. Dass der Begriff "deutsches Internet" an sich schon ein Widerspruch ist, stört die Bezirksregierung genauso wenig wie der Vorwurf der Zensur.

Sicherlich – die Absichten der Bezirksregierung sind bestimmt löblich. Man möchte rechte Nazi-Idioten bekämpfen*. Nur die Methoden sind welche, die das Ende keineswegs rechtfertigen.

Dies bringt die Demonstration natürlich in eine schwierige Argumentationslage. Man möchte nicht in den Verruf geraten, rechte Propaganda zu unterstützen. In der Pressearbeit ist dies gelungen, unter anderen durch das Motto "Wegfiltern ist Wegschauen", welches darlegt, dass die Demonstration keineswegs alles, was im Netz zu sehen ist, gut findet, Filterung jedoch keine Lösung darstellt.

Eine Demo? Offline? Sind die 80er nicht vorbei?

Sicherlich eine berechtigte Frage. Ziel der Demonstration war es jedoch, Öffentlichkeit zu schaffen. Die Bezirksregierung war bisher nicht gerade bemüht, diese Öffentlichkeit selber herzustellen. Mit der Demo kam jedoch die Presse. Und die war ziemlich neugierig. Jede grössere Tageszeitung berichtete.

Zunächst standen nur vier Neonazi-Seiten auf der Zensurliste (davon ist eine bereits offline). Die Provider richteten daraufhin eine DNS-Sperre ein. Die genannten URLs wurden einfach nicht mehr von den Provider eigenen DNS aufgelöst. Sicherlich simpel zu umgehen – aber das stört die Bezirksregierung vorerst nicht. Für 80% der Internetkunden reicht dies, so liess der Medienreferent Herr Schütte verlauten. Vorerst. Die Bezirksregierung möchte eigentlich eine professionellere Lösung für viel mehr zu sperrende URLs, davon nur ein Bruchteil Nazi-Seiten, der Rest eingestuft als 'gefährdend'. Natürlich legt die Bezirksregierung fest, was für sie gefährdend ist und was nicht. Zur Entwicklung dieses Filters wurde eine Expertenrunde einberufen. Die Firmen Bocatel und Webwasher traten an, Zensurprodukte zu entwickeln, und diese an der Uni Dortmund testen zu lassen. Frist: Ende April.

Never forget the Verpeilungsfaktor

Ende April hatte es die Firma Bocatel dann doch nicht gebacken bekommen, auch nur eine Zeile ihres "Filterpiloten" zu programmieren. Die Uni Dortmund, die eigens ein Testlabor (ganze drei Rechner: einen Client, einen Zensurrechner und ein Webserver) eingerichtet hatte, um die Zensurprodukte zu evaluieren, wartete vergeblich auf die Lieferung der Software. Einziges Ergebnis der Tests: "Im Prinzip müsste das Konzept der Firma Bocatel funktionieren" liess der Vertreter der Uni Dormund auf einer Pressekonferenz der Bezirksregierung verlauten, der ansonsten einen Router als "In-Out-Server" bezeichnete. Der Experte stellt sich vor, dass ein zentraler Zensurserver (zum Beispiel im Keller der Bezirksregierung) für alle Internetprovider diese Filtermassnahme durchführen könnte. Herr Büssow, sichtlich beglückt von der Vorstellung, Zensur in seinem eigenen Keller durchführen zu können, verkündete daraufhin, dass er eine Liste von 6000 URLs habe, die er gerne filtern möchte. Verglichen mit der ersten Forderung von nur vier rechtsradikalen Internetseiten ist dies eine enorme Steigerung. Interessant auch, dass dem Verfassungsschutz nur ein Zehntel soviel rechtsradikale Seiten bekannt sind. Achja, nun möchte Herr Büssow auch gegen uns vorgehen – gegen alle die eine Anleitung zur Zensurumgehung veröffentlichen.

Links

- Seite der Demo *http://www.netzzensur.de*
- Unterschriftenaktion *http://odem.org/informationsfreiheit/*
- Hintergrundinformation: *http://www.ccc.de/censorship/*
- Online-Zensurwunschliste der Bezirksregierung: *http://www.bezreg-duesseldorf.nrw.de/cat/SilverStream/Pages/themenframe? Beitrags ID=2071*

Der Herr Büssow, wie er sich über seinen Preis freut: die "Rote Karte".

* Die Redlichkeit der Absichten der Bezirksregierung Düsseldorf sind keinesfalls erwiesen – ebensogut könnte es sich hierbei um einen "lokalen Versuchsballon mit populistischem Vorwand" handeln, der den Weg zur grundsätzliche Contentfilterung ebnen soll. [Anm. d. Red.]

Wie effizient ist Zensur?

von Horst-Walter Schwager

Wer erinnert sich noch an die ersten Zensurversuche im Internet? Der Versuch, das Wort "Breast" (Brust) aus den Usenet-Foren bei Compuserve zu verbannen und die Versuche der deutschen Staatsanwaltschaft, den Zugang zur Zeitschrift "Radikal" auf dem niederländischen Server XS4ALL zu blockieren. Beides in den Jahren 1996 und 1997.

Nach einem fürchterlichen Hin - und Her und nachdem sich die damals schon alte Weisheit von John Gilmore "The Internet treats censorship as a routing problem, and routes around it."[1] mit der blitzschnellen Installation von über 40 Mirrors bewahrheitet hatte, wurde es still um die Herren Kontrolletties. Aber kein Fehler ist dämlich genug, als das er nicht Nachahmer fände und so erfand ein kleiner Provinzfürst im fernen Nordrhein-Westfalen das Rad neu – sozusagen inklusive Holzwurm und Speichenbruch [2,3]. Nach dem Motto "Wir tun was" setzte er voll auf die populistische Schiene Rechtsradikalismus, ließ aber schnell durchblicken, dass sein Modell der Sperrung von Inhalten im WWW ausbaufähig sei und er von der Sperrung "aller verbotenen" Inhalte träume. Ließen wir einmal alle grundsätzlichen Bedenken beiseite und stellten als Bürger die einfache, ja auch in der Politik so beliebte Frage nach der *Effizienz* der Maßnahme, so könnte man sich an einem kürzlich publizierten Artikel von Bruce Schneier [4] orientieren, der diesselbe Frage für Sicherheitsprodukte - und Programme stellte. Schneier hatte sich beklagt, dass Sicherheitsmaßnahmen meistens *ohne* eine vorher/nachher Ananalyse und vor allem ohne Risiko- gegen Kostenabschätzung der Maßnahme durchgezogen werden.Speziell nach dem 11.September... Dies läßt sich denke ich auch auf das Zensur-Thema übertragen:

1) What problem does it solve? 2) How well does it solve the problem? 3) What new problems does it add? 4) What are the economic and social costs? 5) Given the above, is it worth the costs?

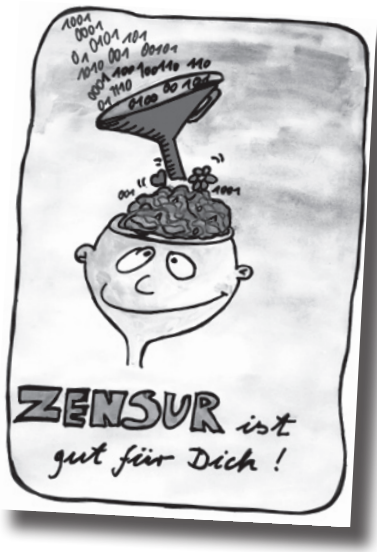
Und ich füge noch hinzu: *6) Which alternatives can be used instead?* Dann läßt sich zu den fünf Punkten Folgendes feststellen:

1) "What problem does it solve?"

Angeblich wird durch die Sperrverfügungen an ISP's der Zugang zu in Deutschland strafbaren Inhalten durch deutsche Bürger (zunächst in NRW) verhindert. Vorgesehen sind Manipulationen des DNS, Zwangs-Proxies und IP-Sperren. Die reklamierten Ziele sind Jugendschutz, Opferschutz, später erweitert auf das Ausfiltern aller "verbotenen" Inhalte. Wer sich auch nur rudimentär mit der Technik des Netzes auskennt sieht, dass die ins Auge gefaßten technischen Sperren wirkungslos sind, da sie umgangen werden können (im Falle der DNS-Manipulation sogar besonders leicht [5]). Damit ist aber auch das soziale Schutzziel, so fragwürdig es auch sei, nicht mehr erreichbar.
In Wirklichkeit wird kein einziges Problem gelöst, vielmehr nur Neue geschaffen (siehe 3-5).

2) "How well does it solve the problem?"

Garnicht: Einmal sind Manipulationen der DNS-Server durch die Auswahl alternativer Server kinderleicht umgehbar und andererseits ist die IP-Sperre ganzer Zielserver durch die Anwahl eines ISP außerhalb von NRW – sollte dieses Modell bundesweit eingeführt werden auch außerhalb der BRD – ebenfalls umgehbar. Eine Zensur ließe sich dann nur noch durch Kappen internationaler Telefonleitungen durchsetzen. Darüber hinaus bleiben für die inkriminierten Informationen alle anderen Transportkanäle offen: Rundfunk, Fernsehen, Zeitschrift, Buch, Telephon, persönliche Kontakte (Versammlungsfreiheit).



3) "What new problems does it add?"

A) Einführung einer durch das Grundgesetz aus sehr gutem historischen Grund verbotenen Zensur (*)[6]. Außerdem werden das Fernmeldegeheimnis gebrochen [7], sowie das ebenfalls im Grundgesetz zwingend vorgeschriebene Zitiergebot [8]. Ferner ist der Mediendienstestaatsvertrag, auf den sich Büssow beruft, garnicht einschlägig, da er nur für Inhalteanbieter gilt. Die Sperrverfügungen ergingen aber ausschließlich an Service-Provider, die Daten nach Teledienstegesetz/ IuKDG nur durchleiten, sie aber nicht auf eigenen Servern vorhalten. Das Teledienstegesetz kennt keine Haftung für Inhalte.

B) Ungleichbehandlung der Gesperrten, denn es werden natürlich bei dem Umfang des WWW nie alle in Deutschland verbotenen Angebote erfaßt.

C) Fehlen jeglicher demokratischen Kontrolle und eines Rechtsweges für die Betroffenen: Der gesperrten Informationsanbieter (die von der Sperre garnicht erfahren dürften) und uns, den zensierten Rezipienten.

D) Aufladen von teuren Überwachungsaufgaben auf die Privatwirtschaft, wo eigentlich der Staat zuständig wäre. Im Ergebnis also eine massive Behinderung der gesamten Informationsgesellschaft und damit auch des "Standortes Deutschland".

4) "What are the economic and social costs?"

"Economic": Finanzierung einer Überwachungsstruktur bei der Behörde selbst und bei den ISP's. Bei Letzteren fallen Kosten für Hardware, Personal, Prozesse und Kundenverluste durch Abwanderung an. Außerdem riskieren zensierende ISP's, die öffentlich "Internet" anbieten Betrugsklagen und Abmahnungen durch Wettbewerber. Risiko der Fragmentierung des Internets und Auseinanderfallens in isolierte Einzel-Ländernetze; also ein drohender Rückfall in vor-Internetwork Zeiten.

"Social": Massive Störung des Rechtsfriedens, Vertrauensverlust in staatliche Organe, jahrelange Prozesse durch alle Instanzen. Internationaler Ansehensverlust. Schaffung eines gefährlichen Präzedenzfalles: Wann wollen iranische Behörden deutsche Server wegen Inhalten iranischer Oppositioneller sperren und wann die Israelis deutsche Server mit Inhalten arabischer Organisationen? Und: Verhinderung von Auseinandersetzung mit neuen, sowie Aufarbeitung des Werkes alter Nationalsozialisten.

5) "Given the above, is it worth the costs?"

Antwort I: Für den, der lesen und denken kann, sowie gutwillig ist ist die Antwort klar!

Antwort II: Da die Sperrverfügungen, die angeblich zum Schutz unserer demokratisch verfaßten Werte erlassen wurden, im Ergebnis genau diese Werte abschaffen würden, ist die Antwort ebenfalls NEIN. Der drohende Kollateralschaden ist für die Gesellschaft untragbar und dies gilt sowohl ökonomisch, als auch - viel wichtiger - sozial! Die Umsetzung und Tolerierung der Sperrverfügungen wäre ein erster Schritt zur Installation einer umfassenden Zensurinfrastruktur an deren Ende auch die Abschaffung der Freiheit steht.

6) "Which alternatives can be used instead?"

A) Argumente und persönliches Vorbild im Umgang mit gefährdeten Menschen und dem Andersdenken.

B) Einbringen der eigenen Werte und Überzeugungen ins Netz, Schaffung von Alternativen zu den Rattenfängern.

C) Erlernen und Lehren der Technik des Internets und seines Kulturraumes. Bereitschaft, Arbeit zu leisten und als Multiplikator zu wirken.

D) Auseinandersetzung mit und Wertung von Inhalten und Kommunikation im Netz. Sich Erarbeiten der Sequenzen: Daten → Information → Wissen → (Weisheit) Suchen → Finden → Bewerten → Einordnen → Erwerb von Medienkompetenz.

E) Setzen auf den mündigen Bürger und Abschaffen des Blockwarts.

(*) Der Begriff "Zensur" wird hier nicht ganz korrekt gebraucht, denn der Verfassungsgeber spricht von einer verbotenen Vorzensur des Publizisten, nicht des Rezipienten. Ich bin aber der Meinung, dass der Mann auf der Straße, für den u.a. der CCC am 06. April 2002

demonstriert hat, ein gutes Gespür dafür hat, was unter einer virtuellen Augenbinde zu verstehen ist: nämlich Zensur :-).

Quellen zur Informationsfreiheit und Zensur:

- Artikel 5 Grundgesetz Aktuell

(1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.

(2) Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre.

- Artikel 19,2 des "Internationalen Pakts über bürgerliche und politische Rechte (ICCPR)"

vom 19. Dezember 1966 [9], dem Deutschland 1973 beigetreten ist, legt fest:

"Jedermann hat das Recht auf freie Meinungsäußerung; dieses Recht schließt die Freiheit ein, ohne Rücksicht auf Staatsgrenzen Informationen und Gedankengut jeder Art in Wort, Schrift oder Druck, durch Kunstwerke oder andere Mittel eigener Wahl sich zu beschaffen, zu empfangen und weiterzugeben."

- Websiten, die Gesetze zum Onlinerecht bereit halten [10,11,12]

- K.Koehntopp: "Why Internet Content Selection and Rating does not work."[13]

- Entschließung des EU-Parlaments gegen Website-Sperrungen [14]

- "Allgemeine Erklärung der Menschenrechte" der Vereinten Nationen [15]: Artikel 19: "Jeder hat das Recht auf Meinungsfreiheit und freie Meinungsäußerung; dieses Recht schließt die Freiheit ein, Meinungen ungehindert anzuhängen sowie über Medien jeder Art und ohne Rücksicht auf Grenzen Informationen und Gedankengut zu suchen, zu empfangen und zu verbreiten."

- Demonstration gegen Netzzensur [16],

Erklärung gegen die Einschränkung der Informationsfreiheit mit Unterschriftenliste [17], Informationen zum Thema Netz und Gesellschaft [18].

(*) wofür ich Belege liefere, wenn erforderlich. Es gibt Hinweise, dass Sie diese Überumpelungstaktik nur anwenden, weil Sie genau wissen, dass Sie mit Ihrem Anliegen vor ordentlichen Gerichten scheitern müssen.

Quellen

[1] *http://www.cygnus.com/~gnu/*

[2] *http://www.brd.nrw.de/cat/SilverStream/Pages/einthema?BeitragsID=180&htid=33*

[3] *http://www.brd.nrw.de/cat/pdf/39sperrverf_022002.pdf*

[4] *http://www.counterpane.com/crypto-gram-0204.html#6)* "How to think about security" B.Schneier ist amerikanischer Kryptologe.

[5] *http://www.ccc.de/censorship/dns-howto/index.html*

[6] *http://www.artikel5.de/artikel/sperrunginffreiheit.html*

[7] Artikel 10 GG, §85 Telekommunikationsgesetz, §206 StGB

[8] Artikel 19 GG

[9] *http://www.heise.de/tp/deutsch/special/frei/12314/1.html*

[10] *http://www.iid.de/rahmen/*

[11] *http://www.online-recht.de/es.html*

[12] *http://www.netlaw.de/gesetze/index.html*

[13] *http://www.koehntopp.de/kris/artikel/rating_does_not_work/index*

[14] *http://fx3.de/shortcut/020220.html, http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/jk-12.04.02-004/default.shtml&words=Sperrung, http://www.europa-digital.de/euonline/policies/politik/epzensur.shtml*

[15] *http://www.uno.de/menschen/menschenrechte/udhr.htm*

[16] *http://www.netzzensur.de*

[17] *http://www.odem.org*

[18] *http://www.schwager.net/gesellschaft.htm*

Weiterführende Links

[1] http://www.netzzensur.de

[2] http://www.odem.org

[3] http://www.schwager.net/gesellschaft/zensur/büssow.htm

[4] http://www.heise.de/chat/archiv/02/04/15/

[5] http://www.brd.nrw.de/cat/SilverStream/Pages/presseframe?BeitragsID=7394

[6] http://www.artikel5.de/home.html

[7] http://www.artikel5.de/artikel/sperrunginffreiheit.html

[8] http://www.nizkor.org

[9] http://www.bocatel.de/filterpilot/

[10] http://www.schwager.net/gesellschaft.htm

Anna Kournikova Deleted by Memeright Trusted System

JAKARTA, December 6, 2067 – Local officials today confirmed that celebrity guru Anna Kournikova died on Wednesday from injuries sustained when a satellite designed to protect intellectual property rights attempted to 'delete' her. "Ms. Kournikova was apparently struck by a powerful, focused beam of microwaves, and died almost instantly," noted Detective J. Sini of the Jakarta Police. "Our current understanding is that this beam issued from one of the MEMEye satellites and that it was an unfortunate accident. We offer our sympathy to her families and followers."

The MEMEye system, activated only last year by international media industry group MPRIAA, is a network of Low Earth Orbit satellites designed to "police traffic in non-digital goods which infringe the memerights of our member artists, producers, and rights owners." The individual satellites, in conjunction with MPRIAA computers, monitor all public activity within their field of view, searching for 'knock-off' products. When the system locates a potentially infringing object, it attempts to query a special chip embedded in protected products. If it receives an inadequate response, the satellite uses a "surgically focused beam" to "delete" the infringing object.

MPRIAA spokesman Ray Insult explains: "Knock-off and pirated products cost designers and artists billions in lost revenues each year. MEMEye protects artists from having their work stolen. Sure, I could still buy a knock- off Mickey, but, as soon as I take it out in public, *thhhhht*, it's gone. That re-balances the market, giving legitimately licensed products a clear value edge over knock-offs."

Kournikova, a member of MPRIAA, had registered to use the system to protect rights in her likeness, including its use in action figures, stuffed dolls, and animatronic facsimiles. "We've had quite a problem with people selling dolls and figurines that look like Anna without paying the licensing fee," notes Kournikova's agent Mercedes Tick. "[MPRIAA] assured us MEMEye was safe."

"In the case of the protection of likeness rights, we take special measures to ensure the safety of our members, but we rely on their cooperation," explains MPRIAA Head of Engineering Eric Themo. "Each member with likeness protection is injected with a subcutaneous chip that informs MEMEye that they are not an infringing likeness. The chip, in effect, gives them a license to use their own likeness, but, when we configure the chip, we depend on the member to give us information about what sort of license they need. I suspect that Ms. Kournikova's license was not configured to permit her use of her likeness in the Asia/Pacific Zone. It would have been a simple matter for us to reconfigure her license for that Zone, if she'd only told us of her travel plans."

Critics of MPRIAA and MEMEye have been quick to point to Kournikova's death as a symptom of the excessive protections rights-holders enjoy under current laws. "Memeright law is so restrictive now that it permits rights-holders, with the help of a private industry group, to punish themselves for violating their own rights," opines Open Meme Initiative founder Phil Pour. "If that doesn't tell you how much lockjaw the law has imposed on the public domain, I don't know what would."

"We are aware of the criticisms," responds MPRIAA's Insult, "and in designing MEMEye we made a conscious choice to continue to permit use of infringing goods in exclusively private spaces. If a kid draws a picture of Mickey at home, and the folks put it up on the fridge, MEMEye won't do anything about that. It doesn't look into your home. It doesn't look through the roofs of buildings. By limiting MEMEye in this way, we protect the legitimate private-use rights of meme users everywhere."

http://www.futurefeedforward.com/

Jugendschutz – Vorwand für massive Zensurmassnahmen?

von Christine Ketzer, Medienpädagogin

An der Front der Jugendschützer weht ein neuer Wind. Dachte man noch vor einem Jahr beim Besuch entsprechender Tagungen und Anhörungen, die Jugendschützer- und Bewahrpädagogenszene hätte dazugelernt, wird man nun aufgrund massiver Zensurversuche seitens der nordrhein-westfälischen Landesregierung eines besseren belehrt.

Die Situation: verschiedene Provider in Nordrhein-Westfalen haben auf Druck der Landesregierung einige als jugendgefährdend oder politisch inkorrekt eingestufte Seiten gesperrt. Sicher, diese Seiten sind unbestritten nicht die Krone der Publikationen im World Wide Web, dennoch ist nicht einzusehen, dass diese Seiten für einige Bürger Nordrhein-Westfalens, darunter auch Studenten mancher Universitäten, nicht mehr anzusehen sein sollen. Insbesondere die im Grundgesetz festgelegte Freiheit der Forschung und Lehre wurde hier geflissentlich ignoriert. Bekannt ist, dass dieses Grundrecht durch das Jugendschutzgesetz beschränkt wird. Und damit wird ein Verdacht erhärtet, der sich schon lange aufdrängt, nämlich dass der Jugendschutz immer dann herhalten muss, wenn gesellschaftlich unliebsame Inhalte aus dem Internet verbannt werden sollen. Gemeinhin ist das als Zensur zu werten.

Die Argumentation ist, und das kann ich durch den Besuch mehrerer Fachtagungen und Kongresse untermauern, immer gleich. Verläuft die Diskussion anfänglich noch auf sachlicher Ebene, wird sie doch nach kurzer Zeit durch die Befürworter staatlicher Zensur auf eine emotionale Ebene verschoben, auf der man in einer Powerpoint-Präsentation die gesammelten Scheusslichkeiten des Webs aufzeigt, man Reizwörter wie "Kinderporno" oder "Rechtsextremismus" fallen lässt und so in jedem "rechtschaffenen" Menschen Abscheu und Ekel hervorruft und den Wunsch nach Beseitigung dieser Inhalte laut werden läßt.

Auch als Gegner staatlicher Zensur ist man diesen Inhalten in der Regel nicht zugeneigt, weiß jedoch auch, dass aus wissenschaftlichen Studien hervorgeht, dass Filter nicht den gewünschten Effekt zeigen (z.B. Copa Commission-Untersuchung der US-Regierung) und eher kontraproduktiv sind.

Doch es ist dann meist schon zu spät, eine sachliche Diskussion auf wissenschaftlicher Ebene weiterzuführen, denn wo Schutzinstinkte einmal geweckt wurden, kann man auch mit noch so renommierten Studien nichts mehr bewirken. Dort geht es um Emotionen, nicht um Fakten.

Sicher darf man es sich bei dieser Thematik nicht einfach machen, denn es gibt für diese komplexen Fragen keine einfachen Antworten, wie das Sperren einiger Seiten oder Teile ganzer Dienste.

Das Problem entstand nicht erst gestern, doch wie immer wurde es im Vorfeld versäumt, Forschung im Bereich der Medienpädagogik voranzutreiben und Lehrer, Pädagogen und Erziehungsberechtigte auf die Begleiterscheinungen, der im Bereich der Wirtschaft massiv unterstützten Wissensgesellschaft, vorzubereiten. Doch dieser Zug ist bereits abgefahren. Die Ausbildung an den Hochschulen ist im Bereich der Medienpädagogik rudimentär und allein in meiner Studienzeit wurden zwei Lehrstühle für Medienpädagogik (Köln und Bonn) nicht wieder besetzt.

Dass Lehrer und Erziehungsberechtigte überfordert sind, wundert nicht. Doch welche Lösungen gibt es auf Seiten der Zensur-Gegner für das herrschende Dilemma?

Mit Kommentaren wie: "Das kann man doch eh alles technisch umgehen" ist es nicht getan, denn ein Großteil der Bevölkerung wird die Zensurmaßnahmen eben doch nicht umgehen können und ein freies Internet nur für wenige Technik-Freaks kann nicht unser Ziel sein. Das Problem ist, wie schon erwähnt, komplex und muss auch so behandelt werden.

Meist sind es einfache Dinge, die viele Probleme lösen können. Ein paar Ansätze seien hier, auch aus meiner eigenen zweijährigen Praxis als Leiterin eines Internet-Cafés für Jugendliche aufgeführt:

Räumliche Lösungen

Allein durch die Anordnung der PCs lassen sich Übertretungen des Jugendschutzgesetzes recht gut verhindern. In einer Reihe hintereinander angeordnete Rechner laden zum Besuch altersungeeigneter Seiten förmlich ein. Eine Anordnung der Rechner im Halbkreis, so dass die Rechner von der Aufsichtsperson eingesehen werden können, ist meist schon die Lösung vieler Praxisprobleme.

Festlegung klarer Regeln

Im Bereich von Internet-Cafés, wie auch in der Schule und zuhause, sind klare Absprachen das A und O. Es muss deutlich gemacht werden, wo die Grenzen der Internet-Nutzung liegen und aus welchen Gründen diese gesetzt werden. Die Grenzen können innerhalb des Jugendschutzgesetzes recht weit gesteckt sein, sollten aber auch verbindlich eingehalten werden.

Berücksichtigung des Alters

Viele Eltern und Pädagogen scheinen mehr von seitens der Wirtschaft geforderten "Technikkompetenz" geleitet zu werden, als von dem was ihr Kind im jeweiligen Alter bereits verarbeiten kann. Das Internet bietet viele Möglichkeiten und nahezu alle Inhalten, die man sich vorstellen kann, dass Kinder in einem bestimmten Alter mit der Fülle des Angebotes überfordert sind oder noch nicht einschätzen können, was für sie geeignet ist, sollte einsehbar sein. Es ist auch nicht Aufgabe der Kinder, solcherlei zu entscheiden, sondern die der Erziehungsberechtigten. So wie Eltern eine Verantwortung für den Besuch anderer öffentlicher Bereiche (wie z.B. Discos etc.) tragen, haben sie auch eine Verantwortung für den Medienkonsum ihrer Kinder. Eltern sind an dieser Stelle nicht alleine zu lassen, sondern z.B. durch entsprechende Portalseiten speziell für Kinder, an die Hand zu nehmen und zu beraten.

Aufklärung der Bevölkerung

Wünschenswert wäre im Rahmen der Information der Bevölkerung auf eine ausgewogene und der Realität entsprechende Darstellung der Internetdienste zu setzen. Die reißerisch und teils sachlich falschen Darstellungen in manchen Medien tragen nicht dazu bei, sich ein differenziertes Bild über Nutzen und Risiken des Internets zu machen. Sicherlich wird es solch eine Berichterstattung immer geben, dennoch kann man dem etwas entgegensetzen und die Menschen über Gefahren, insbesondere im Bereich des Datenschutzes, aufklären. Nötig sind auch öffentliche Diskurse, wie man mit unliebsamen Inhalten umgehen kann, um einem Gefühl der Machtlosigkeit entgegen zu wirken.

Es gibt mittlerweile ausreichend Meldestellen (z.B. *http://www.fsm.de* oder *http://www.jugendschutz.net*), an die man sich wenden kann. Content-Provider sind in der Regel durch Datenbankabfragen bei den nationalen Network Information Center (wie z.B. DENIC) zu ermitteln. Der Mythos vom anonymen Anbieter, dem man nicht beikommen kann, sollte demontiert werden. Die meisten Content-Provider sind durch Domain-Abfragen oder andere einfache Programme (Ping, Traceroute) zu ermitteln.

Strafrechtliche Verfolgung

Netzinhalte, die unter das deutsche Strafrecht fallen sind entsprechend zu verfolgen. Die zuständigen Behörden sind besser über die Gegebenheiten des Netzes zu informieren.

Zusammenfassend gilt: Kinder und Jugendliche sind ihrem Alter entsprechend ins Netz zu "entlassen", gegebenenfalls nur in Begleitung ihrer Eltern, diesen sind entsprechende Hilfen zu geben.

Eine zentrale Sperrung einiger Webseiten, die dann auch für die erwachsene Bevölkerung nicht mehr zugänglich sind, ist nicht akzeptabel. Die alte Frage "Wer kontrolliert die Kontrolleure?" hat in diesem Zusammenhang neue Aktualität. Wenn es überhaupt zu Zensur kommen muss, so hat diese am heimischen Endgerät zu erfolgen, nicht aber in staatlichen Einrichtungen.

Jugendschutz darf nicht als Vorwand für das Wegschalten gesellschaftlich unerwünschter Tabuthemen herhalten. Er hat seine Berechtigung und muss mit wirksameren Methoden (s.o.) durchgesetzt werden. Auf dem Weg in die sogenannte "Informations- und Wissensgesellschaft" dürfen wirtschaftliche Interessen nicht vor denen der Bevölkerung stehen. Die Politik muss das in ihren Entscheidungen berücksichtigen und darf nicht den Fehler begehen, alte, bisher auch nur unzureichend funktionierende Maßnahmen, auf das Netz zu übertragen.

Aus unserer beliebten Reihe "Was Nerds im Urlaub so alles photographieren" diesmal "Strommast in Tokyo" von Tina

Happy Volksverarschung

von Dr. Sarah Spiekermann

Fast jeder deutscher Bürger, sei es beim Erhalt seiner Telefonrechnung oder bei einer Fahrt mit der Bahn, wird in den letzten Monaten dazu animiert, an Bonusprogrammen teilzunehmen: Punkte und Rabatte locken bei vielen Unternehmen – der Telekom, der Bahn, bei Karstadt, Payback-Partnern oder der Lufthansa. Mitmachen bedeutet, so wird es kommuniziert, zum privilegierten Kundenkreis aufsteigen, Spaß haben beim Punktesammeln und -verwalten und vor allem beim Einlösen attraktiver Prämien, die vom Kulturbeutel bis zum Wellnesswochenende alles bieten.

Wer den verwunderten Schaffner auf jeder Bahnfahrt von neuem davon überzeugen muss, dass er ausnahmsweise mal keine Punkte will, kommt sich schon richtig komisch vor. Warum plötzlich all diese Bonusprogramme? Warum eine Kundenkarte für jeden Laden, den man betritt?

Folgt man als Konsument den Aussagen der Programmbetreiber so entsteht der Eindruck, dass Unternehmen vor allem die Treue von guten Kunden belohnen möchten, ihren Kunden mehr Spaß beim Konsum schenken möchten und beim Befriedigen der eigenen Sammelleidenschaft, ein neuer Service eben, der Prämien und privilegierte Behandlung verspricht. Wenn man sich die angebotenen Programme jedoch näher anschaut und das hinterfragt, was dem Kunden hier in so netter und teurer Verpackung angetragen wird, so ist man doch leider häufig schnell ernüchtert. Wer beispielsweise bei der Deutschen Telekom in das HappyDigits-Programm einsteigt, muss schnell feststellen, dass er bei Erhalt von 1 Digit pro ausgegebenem Euro lange Punkte sammeln muss, bevor er sich mal eine Prämie zusammengespart hat. So zum Beispiel der mit 1000 Digits veranschlagte JoJo. Um ihn zu bekommen braucht ein Telekom Festnetzkunde mit einer doch ordentlichen Telefonrechnung von rund EUR 50 im Monate (EUR 24,75 T-ISDN Standardanschluss und EUR 25 Gesprächsumsatz) und unter Berücksichtigung der 50 Geschenkpunkte beim Programmeinstieg genau 3 Jahre und 2 Monate bis er ihn sich zusammengespart hat. Dabei ist noch nicht berücksichtigt, dass ab Beginn des 3. Teilnehmerjahres die ersten Punkte schon wieder verfallen und der Kunde wirklich noch länger braucht, bis er endlich zu seinem JoJo kommt, falls dieses denn dann noch als Prämie zur Verfügung steht. Angenommen der Kunde ist ein wirklich besonders guter Telekom-Kunde und bezieht auch seinen mobilen Anschluss vom Unternehmen durch die T-Mobil, wo er nochmals für EUR 25 telefoniert. Dann braucht er aber immer noch 1 Jahr und 7 Monate für das Jojo. Für die Erarbeitung einer interessanteren Prämie hingegen, zum Beispiel eines DVD-Players (43.500 Digits) auf diesem Wege hingegen 71,6 Jahre. Von dem Wellnesswochenende in Potsdam (79.270 Digits) kann der Kunde leider erst in 131,3 Jahren, also lange nach seinem Tod profitieren. Pech gehabt. Eine echte Belohnung für den treuen Kunden? Oder wirklich nur noch Verarschung desselbigen?

Möglicherweise, so könnte argumentiert werden, hat hier einfach die zuständige Marketingabteilung der Telekom beim Programmdesign versagt. Ein schlechtes Anreizsystem, wo von einem ‚Profitieren' des Kunden, wie es die Webseite verspricht, wohl kaum die Rede sein kann. Aber das bedeutet ja noch lange nicht, dass Bonusprogramme generell kundenunfreundlich sind. Immerhin gibt es international und in Deutschland ja auch sehr erfolgreiche Treueprogramme, vor allem bei den Fluglinien, wo man sich nach 30 Inlandsflügen auch schon mal über die Jahre hinweg einen Gratisflug erarbeiten kann und wo eine Meile, Punkt oder Digit unter Umständen bis zu 9 Cent wert ist (statt 1 Cent bei der Telekom) und auch nicht verfällt. Betrachtet man jedoch das zweite derzeit in Deutschland lancierte Punkteprogramm der Bahn, so entdeckt man auch hier, ähnlich wie bei HappyDigits, fragwürdige Programmcharakteristika:

Für so manchen, der am Serviceprogramm für Vielfahrer bahn.comfort mitmacht, scheint zunächst die Punktezahl noch erreichbar, die man braucht, um zum erlauchten Kundenkreis aufzusteigen. Für Erwachsene mit einer 2.-Klasse-Bahncard (für die immerhin EUR 140 bezahlt werden) ist es zum Beispiel möglich (nach gegenwärtigem Tarifschema), unter der Voraussetzung, dass keine Sparpreise, Guten-Abend- oder Familientickets genutzt werden, sich durch nur 41 Fahrten Düsseldorf – Hannover innerhalb von sechs Monaten den Komfortstatus zu erarbeiten. Abgesehen davon, dass die Anzahl der nötigen Fahrten innerhalb eines so kurzen Zeitabschnitts

immer noch relativ viel erscheint, ist jedoch sehr viel kritikwürdiger, was dem treuen Vielfahrer und Nichtflieger dann als Gegenleistung geboten wird. Sachprämien, z.B. die Ersammelung einer Gratisfahrt (analog zu den Fluglinien) werden jedenfalls nicht geboten. Stattdessen bietet man dem Kunden garantierte Sitzplatzreservierung und Sitzplatzbereich. Fraglich ist jedoch, wie häufig es wirklich vorkommt, dass man keinen Sitzplatz mehr bekommt, wenn man ohnehin während der Geschäftszeiten fährt und wie wichtig es ist, physisch nun auch neben einem anderen Vielbahnfahrer platziert zu werden. Das Servicetelefon, welches sich zunächst so anhört, als könne man hier umsonst Tickets buchen und Reservierungen vornehmen, entpuppt sich als eine Telefonnummer, wo es nur Auskünfte zum Programm gibt, sonst nichts. Wie das mit den extra Parkplätzen für Komfortkunden aussieht kann auch die Bahncard-Service-Auskunft nicht so richtig sagen. Die soll es wohl mal geben, aber wo und wie viele und ob man dann sein Zugticket ins Autofenster legen soll oder die Bahncard (was ja wohl nicht geht), das weiß man hier auch noch nicht so recht. DB-Lounges jedenfalls gibt es wohl an jedem größeren Bahnhof, meint zumindest das Servicetelefon. Aber das Essen ist hier auch nicht umsonst. Da kann man doch gleich ins nächstgelegene Lokal gehen. Bleibt letztendlich nur noch das kostenfreie Partizipieren am RAILPLUS-Angebot für die vielen Auslandsreisen, die man heute noch mit der Bahn macht. Dieses müsste man sonst gegen 15 Euro extra für die Bahncard erwerben. Ja und natürlich, dass gute Kunden keine halbe Stunde mehr warten müssen, um ein Ticket an den überfüllten Verkaufsschaltern zu bekommen. Aber mal ganz ehrlich: wozu denn eigentlich Punkte sammeln? Damit die wenigen, die es schaffen, dann nicht mehr anstehen müssen?

Die Beispiele legen es nahe, dass eine Belohnung von Kundentreue bei einigen Bonusprogrammen nicht wirklich im Vordergrund stehen kann, kommt doch die Anreizstruktur eher einer Veralberung nahe als einem zusätzlichen Service. Was steckt also wirklich dahinter? Warum plötzlich all diese Programme, die mit solcher Macht beworben und in den Markt gedrückt werden?

In Wirtschaftskreisen ist bekannt, dass die Kundenloyalität in den letzten Jahren stark abgenommen hat. Die Markentreue lässt nach. Um Kunden von einem Wechsel zur Konkurrenz abzuhalten, um sie zu überzeugen, die eigenen Produkte zu kaufen, das wissen heute die meisten Unternehmen, ist es nötig den Kunden pro-aktiver anzusprechen, mit persönlich zugeschnittenen Angeboten auf ihn zuzutreten. Das kann vom personalisierten Otto-Katalog, über den individuellen Onlinebereich bis hin zum Hochglanzpapier für den Premiumkunden reichen, oder aber einen abendlichen Anruf in der Familie bedeuten, um die eigenen Leistungen passend zum Abendessen zu bepreisen. Kunden werden nach ihrem Ausgabeverhalten, nach ihrem Ausgabepotential, ihrem Lebensstadium, kurz, nach ihrem ‚Wert' für das Unternehmen eingeteilt, nach Interessen sortiert und dann möglichst automatisch und im Massenverfahren angesprochen, per Telefon, E-Mail, Postweg oder Fax. Diese, unter dem Schlagwort Kundenbeziehungsmanagement oder auch Customer Relationship Managment (CRM) durchgeführten Praktiken führen bei Unternehmen zu deutlichen Effizienzsteigerungen. Bei professioneller Durchführung kann eine feine Unterteilung der Kundenbasis in hunderte von separaten Segmenten zu einem bis zu dreifachen Return-on-Marketing-Investment führen. Umsatzsteigerungen, vor allem bei personalisierten Onlineangeboten à la Amazon liegen gegenüber nicht personalisierten Angeboten wohl sogar bei bis zu 12%. Für Unternehmen lohnt sich also die personalisierte Kundenansprache.

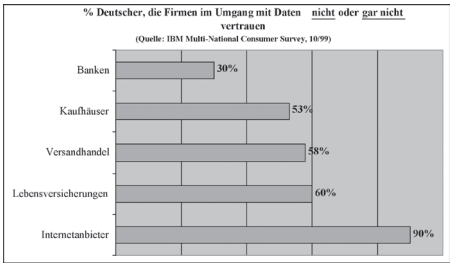
Die Basis für diese Art von Kundenbeziehungsmanagement jedoch ist das Wissen über den Kunden, die Daten und Informationen über ihn, um überhaupt festzustellen, ob er ein guter oder schlechter Kunde ist, was ihn interessiert und ob es sich lohnt, ihn persönlich anzusprechen. Wer bisher ohne Kundenkarte einkaufen ging, der war anonym für den entsprechenden Anbieter. Ein Karstadt wusste nicht, wer wann was in den Warenhäusern einkaufte, wer einen hohen Kundenwert hat und wer nicht. Dank der Kundenkarte ist dies jetzt anders. Name, Anschrift, Telefonnummer und E-Mail, die ja bei der Registrierung für Kundenprogramme abgefragt werden, werden dann genutzt, um die interessanten Kunden zu identifizieren und direkt anzusprechen. Dabei floriert der Markt für Adressdaten nicht nur wegen dieser Kontaktmöglichkeit, sondern auch, um zu verstehen, in welches soziale Milieu man den Kunden denn einzuordnen hat, wie viel er ‚auf der hohen Kante' hat. Die guten ins Töpfchen, die schlechten in Kröpfchen. Firmen wie beispielsweise die *Schober Information Group* leben davon, einer Adresse die entsprechende Wertigkeit der Wohngegend bis auf Straßenebene beizufügen, Häuserebene ist in der Planung. Die Firma wirbt damit, über 50 Millionen Privatadressen und 2,2 Milliarden Zusatzdaten zu verfügen. Wer im falschen Viertel wohnt, sollte sich also nicht wundern, wenn er den bestellten Katalog auch schon einmal nicht bekommt oder im Internet nicht mehr per Nachnahme bezahlen kann. Das fällt dann unter den Terminus des ‚Risikomanagement'.

Um zu verstehen, wer ein Kunden wirklich ist, reicht es Firmen jedoch häufig nicht mehr aus, nur seinen Namen zu kennen, seine Wohngegend oder das Telefonieverhalten zu den Zeiten, wo er HappyDigits benutzt. Wirklichen Einblick in die ‚Psyche' des Kunden erhält man erst, wenn man einen Blick in seinen gesamten Warenkorb werfen kann. Dazu ist es zwangsweise nötig, dass sich beispielsweise ein Telekommunikationsunternehmen, welches nur die Telefonrechnungen der Kunden kennt, Partnerunternehmen zum Datenpooling sucht, welche andere Warengruppen bedienen. So

verwundert es nicht, dass plötzlich in der langen Liste der am HappyDigits-Programm beteiligten Unternehmen eine unscheinbare Partnerfirma mit dem Namen CAP Customer Advantage Program GmbH auftaucht. Wohlgemerkt nicht in der Rubrik ‚Partnerunternehmen', sondern versteckt im Bereich ‚Datenschutz'. Da stellt man dann fest, dass es sich hier wiederum um ein Joint-Venture der Telekom mit KarstadtQuelle handelt. So können dann in Zukunft alle Informationen über das Telefonieverhalten verbunden werden mit sämtlichen Einkäufen der Karstadt-Kundenkarte. Während dieses ‚Rundumeinblickspaket' in die Haushalte bei HappyDigits noch in den Anfängen ist, hat das Payback-Programm mit derzeit 17 Millionen Kunden in Deutschland schon bessere Karten. Potentiell weiß man dort wirklich schon fast alles über den Kunden. Zum Beispiel über Frau Müller, eine 29-jährige Angestellte, die fast immer nur Billigangebote kauft, ob nun in der Galeria Kaufhof oder im Realmarkt, sogar bei der Babynahrung. Alkoholika kauft sie eigenartigerweise nur an der Tanke und auch nicht gerade wenig und auch schon mal unabhängig vom Benzinbedarf. Aber kein Wunder, sie wohnt ja um die Ecke von der Tanke, übrigens eine schlechte Wohngegend. Diese Art von doch recht aussagekräftiger Profilbildung erlaubt einen wunderbaren Einblick in den Haushalt Müller. Möglich ist dann auch eine entsprechende Ansprache und Behandlung: z.B. das systematische Zusenden von Übersichten zu Billigangeboten, vielleicht sogar die billigerer Babynahrung und Hinweise, wo für wenig Punkte die große Prämie geholt werden kann.

Diese etwas drastische Darstellung soll jedoch nicht zu einseitig sein. Ebenso ist es möglich, festzustellen, dass jemand Senator bei einer Fluglinie ist, regelmäßig Luxusgüter über seine Kreditkarte bezieht und gerne in der Toscana Urlaub macht. Folglich bekommt er dann die Hochglanzbroschüre, erreicht das Call Center auf Anhieb und erhält Sonderangebote für Italienflüge. An der Tatsache allein also, entsprechend seines Verhaltens von Firmen eingeordnet und dann auch entsprechend behandelt zu werden, müssen sich Kunden nicht stören, vor allem dann nicht, wenn sie durch ihre Vermögensverhältnisse beglückt, zu den heiß begehrten A-Kunden gehören. Ein großer Teil von rund 40% der Verbraucher sagen laut einer IBM-Studie, dass sie personalisiertes Marketing für eine gute Sache halten. Sie sparen Zeit und können leichter das finden, was sie wirklich interessiert. Auch hört man nicht selten die Meinung, dass es doch egal sei, wenn Firmen viel über einen wissen. Zwar vertrauen viele Kunden Firmen nicht im Umgang mit ihren Daten (siehe Kasten), aber doch scheinen wohl die Zeiten lange vorbei (leider), in denen sich 1983 allein in Hamburg über 50 Bürgerinitiativen gründeten, um sich gegen 10 persönliche Datenangaben im Rahmen der Volkszählung zu wehren.

Die Entscheidung, sich gegenüber den Herties dieser Welt zum ‚gläsernen Menschen' zu machen, ist eine Wahl, die jeder im Rahmen seines Grundrechts auf informationelle Selbstbestimmung treffen kann. Wer sich selbst und sein Leben publik macht, sei es per Web-Cam im Internet, beim Treuetest im Radio, im Big-Brother-Container oder mit Hilfe von Kundenkarten, der mag das tun. Jeder ist der Herr seines Schicksals. Allerdings, und um wirklich Herr zu bleiben, sollte der Bürger in die Lage versetzt sein, die Entscheidung für oder gegen eine Veröffentlichung seines Lebens ‚bewusst' zu treffen. Was Bonusprogramme angeht, sollte er zumindest wissen, wozu diese überhaupt gedacht sind, was in diesem Zusammenhang mit seinen persönlichen Informationen geschieht und in wie fern er zur Teilnahme berechtigt ist, ohne alle geforderten Angaben zu machen. Allerdings hapert die Aufklärung gerade an diesem Punkt. Nichts scheinen Unternehmen so sehr zu fürchten wie die Offenheit und Ehrlichkeit gegenüber dem eigenen Kunden. Ein Beispiel: Wenn man Mitglied im Klub Karstadt werden will und eine SolitaireCard mit Zahlungsfunktion bestellt, werden einem plötzlich zusätzlich zu den Kontaktinformationen Fragen zum Familienstand gestellt. Karstadt will wissen, ob man ein eigenes Haus besitzt oder zur Miete wohnt, ob man in letzter Zeit schon mal umgezogen ist, wie viel man verdient, wie viele unterhaltspflichtige Kinder man hat, was man beruflich macht, in welcher Branche man tätig ist, wie lange schon, was der Partner macht, auch in welcher Branche, bei welchem Unternehmen, wie lange und unter welcher Telefonnummer er erreichbar ist. Tatsächlich hingegen bedarf es für die Überprüfung der Kreditwürdigkeit eines Kunden bei der Schufa nur der Angabe von Name, Anschrift, Geschlecht und Geburtsdatum. Wer nun von den großzügigen 3% Rabatt mit Zahlfunktion bei Karstadt profitieren will, der scheint gezwungen, die Angaben zu machen. Wenn man sie nicht macht, tja, dann weiß auch die freundliche Kundenberaterin sowie die Auftragsbearbeitung des KaDeWe nicht, ob man Mitglied werden kann. Und dies obgleich die Gesetzgebung doch klar ist: Der Grundsatz der Datensparsamkeit untersagt es Karstadt eigentlich, die Daten überhaupt zu erheben.



Aber die scheinbar nötige Erhebung von Informationen zu Marktforschungszwecken ist nur ein Zeichen von fehlender Offenheit gegenüber dem Kunden. Fragwürdig werden die Praktiken, wenn man versucht, den Kunden durch verstecktes ‚Kleingedruckte' aufs Glatteis zu führen. Warum versteckt das HappyDigits-Programm die Tatsache, dass es die eingesammelten Informationen mit dem KarstadtQuelle-Konzern teilt? Warum wird diese für den Kunden wichtige Information nicht unter dem Punkt ‚Partnerunternehmen' aufgezeigt? Warum musste Payback erst von Verbraucherschützern gerichtlich dazu gezwungen werden, die eigenen AGBs datenschutzkonform zu gestalten? Wie kann es sein, dass dieses größte Bonusprogramm Deutschlands den Big-Brother-Award für das datenschutzfeindlichste Unternehmen des Jahres 2000 trägt?

Die Beispiele zeigen, dass wir in Deutschland heute an einem Punkt sind, wo unabhängig von Schutzgesetzen mehr Offenheit im Hinblick auf die Datenerhebung und -verarbeitung gelebt werden sollte. Diese Offenheit könnte zum Beispiel beinhalten, dass Anmeldeformulare zu Bonusprogrammen den potentiell Teilnehmenden verdeutlichen, dass das Programm für die persönliche Ansprache gedacht ist und dass dafür möglichst viele Daten über eine Person gebraucht werden. Wenn die Anreize fair sind, warum sollten Kunden die Angaben nicht machen? Wenn kenntlich gemacht würde, welche Daten prozesstechnisch gebraucht werden (z.B. zur Überprüfung der Zahlungsfähigkeit) und welche man sich zusätzlich wünscht (vielleicht gegen extra Punkte?) könnte der Verbraucher viel bewusster entscheiden, was er sagt und zu welchen Konditionen. Wenn zusätzlich noch eine Anlaufstelle genannt würde (was übrigens nach BDSG vorgeschrieben ist, jedoch einfach von vielen Anbietern ignoriert wird), wo der Verbraucher seine Daten beim Unternehmen ggf. einsehen, ändern oder löschen kann, würde er sich sicherlich noch wohler fühlen, diese von sich preiszugeben.

Kann informationelle Selbstbestimmung überhaupt noch bewusst gelebt werden, wenn man all diese Informationen von Unternehmen nicht bekommt, nicht weiß, zu welchen Angaben man verpflichtet ist und zu welchen nicht? Da wird der Kunde damit gelockt, für oft unerreichbare Prämien sinnlos Punkte zu sammeln und zu verwalten, gezwungen, durch entsprechende Teilnahmebedingungen und verklausulierten Datenschutz seine persönlichen Informationen preiszugeben und letztendlich dazu gebracht, sich in Eigenregie als D-Kunde (Terminologie für ‚schlechter' Kunde) und Schnäppchenjäger zu outen. ‚Schöne Aussichten', ja, damit hat die Prämienbroschüre des Karstadt Klubs sich selbst doch gleich den richtigen Titel verpasst.

Voice over IP

von Lars Weiler <pylon@duesseldorf.ccc.de>

Ein Vergleich zwischen H.323 und SIP

Es wird immer deutlicher, dass der Kommunikation über Datenleitungen die Zukunft gehört. Dafür wurden einige Protokolle entwickelt, von denen zwei aktuell in der Diskussion sind. Ich möchte eine kurze Einführung und einen kleinen Vergleich zwischen den beiden Protokollen geben. Ein sehr ausführlicher Vergleich ist auf den Seiten von *packetizer* [1] zu finden.

H.323

Dieses Protokoll wird in der *ITU-T recommendation H.323* [2] beschrieben. Diese in der Entwicklung 1995 gestartete "Empfehlung" basiert hauptsächlich auf dem H.324-Protokoll. Im Jahr 1996 wurde die Version 1 herausgegeben, welche 1998 von der Version 2 und 2000 von der Version 4 ersetzt wurde (die Version 3 ist nie erschienen). Zu der Philosophie heißt es:

H.323 was designed with a good understanding of the requirements for multimedia communication over IP networks, including audio, video, and data conferencing. It defines an entire, unified system for performing these functions, leveraging the strengths of the IETF and ITU-T protocols. [1]

Im Grunde kann man sagen, dass H.323 in Anlehnung an H.320 ("Bild-Telefon") entstand und ursprünglich eine nahezu 1-zu-1-Übertragung von ISDN auf ein IP-basiertes Netz ist. Im Laufe der Zeit wurden dann einige Merkmale hinzugefügt.

SIP

Das "Session Initiation Protocol" wird im IETF RFC 2543 [3] beschrieben. Dieses Protokoll basiert auf einigen anderen RFCs. 1996 wurde mit der Entwicklung begonnen und 1999 als RFC herausgegeben. Nun wieder ein kurzer Auszug zur Philosophie:

SIP was designed to setup a "session" between two points. It has a loose concept of a call (that being a "session" with media streams), has no support for multimedia conferencing, and the integration of sometimes disparate standards is largely left up to each vendor. [1]

Harte Worte, aber das verwundert nicht, denn es wurde der Versuch gestartet, das Thema IP-basierte Kommunikation völlig anders anzugehen und weg von den Strukturen der jetzigen Telefonnetze zu kommen. Letztendlich basiert SIP auf Protokollen, die ihren "praktischen Test" schon bestanden haben und nicht mehr aus dem Internet wegzudenken sind, wie zum

Beispiel HTTP und E-Mail (um die bekanntesten zu nennen).

Der Vergleich

Beide Standards haben ihre Vor- und Nachteile. Für einen Telefoniediensteanbieter sind solche Punkte wie stabile Leitungswege und ein richtiges Billing vonnöten. Andere Institutionen setzen ihren Schwerpunkt, der für sie VoIP interessant macht, auf abhörsichere Verbindungen oder allgemeine Einsparungen im Telekommunikationsbereich. Ich möchte noch kurz ein kleines Missverständnis aus dem Weg räumen: H.323 und SIP sind keine Dienste, die Audio- und Videodaten kodieren! Sie helfen lediglich beim ordentlichen Verbindungsaufbau und stellen sicher, dass diese Verbindung wieder sauber abgebaut wird oder arrangieren das Mixen von mehreren gleichzeitigen Kanälen, zum Beispiel für eine Konferenzschaltung. Die eigentlichen Codecs sind für beide Protokolle weitestgehend uninteressant.

H.263	SIP
Vorteile	
alles ist vorgeschrieben, inklusive der zu verwendenden Audio- und Video-Codecs	basiert auf existierenden Grundelementen des Netzes, wie URL, MIME oder DNS
integriertes Load-Balancing	Messages sind in plaintext
bestehende VoIP-Produkte basieren meistens auf H.323	schnellerer Verbindungsaufbau
	kann Anrufe "forken" (auf mehrere Endgeräte gleichzeitig leiten)
Nachteile	
Verbindungsaufbau kann mehrere Sekunden dauern	benötigt ein funktionierendes Netzwerk mit einigen Standarddiensten
Messages sind im Binärformat	kein Load-Balancing implementiert
das komplexe System verursacht Mehrkosten und oft Fehler	

Im Grunde kan man sagen, dass H.323 recht stabil ist und einige Netzwerke aufgebaut wurden, jedoch einen ganzen Stapel an weiteren Protokollen der ITU nutzt, die auch nur gegen entsprechendes Entgeld zu erhalten sind – mit dem Ergebnis, dass es sehr komplex wird. Dieses ist ein Grund, warum einige große Hersteller von VoIP-Soft- und Hardware auf SIP umschwenken. Im Gegensatz dazu ist SIP einfacher und flexibler. Jedoch verlangt es mehr "Intelligenz" von den Endgeräten (was heute aber sehr leicht zu bewerkstelligen ist), sodass auf den nötigen Servern für den Verbindungsaufbau weniger Last anfällt.

Unglücklicherweise ist dadurch das Billing schwieriger zu bewerkstellien (jedoch nicht unmöglich), was SIP bisher für Telefoniediensteanbieter uninteressant machte. Einer der genannten Vorteile von H.323 ist, dass es so gut wie alles fest vorschreibt, wodurch es kaum zu Komplikationen beim Verbindungsaufbau kommt (und dennoch gibt es oft Probleme bei der Kommunikation von diversen Clients untereinander). Dadurch, dass es der erste Standard am Markt war, wurden bereits sehr viele Produkte, sowohl Hardware, als auch Software, entwickelt.

Vor allem das nun implementierte Quality-of-Service ist ein großer Vorteil der aktuellen Version 4 der Protokollbeschreibung. Das Billing ist insoweit möglich, dass eine Verbindung nur dann aufgebaut werden kann, wenn sich der Client bei einem GateKeeper (eine Art Nameserver, um IP-Adressen zu Rufnummern oder Aliase zuzuweisen) registriert hat, der dann die Verbindungen loggt und das Billing somit übernimmt. SIP kann ebenso Billing zur Verfügung stellen, es ist aber nicht im RFC beschrieben. Einige Anbieter haben dementsprechend Erweiterungen entwickelt und mittlerweile für gut entschieden.

Dass Programme für SIP relativ einfach geschrieben werden können, liegt an den Plaintext-Messages. Sie können ohne weitere Probleme von z.B. Perl-Programmen verarbeitet werden, wie es schon seit Jahren von E-Mails bekannt ist. Auch Fehlermeldungen können einfach gelesen werden, ohne sie vorher wieder decodieren zu müssen. Somit stellt SIP nicht nur die Grundlage für den Aufbau von Audio- oder Videoverbindungen dar, sondern kann als Instant-Messenger verwendet werden, einen Ersatz für E-Mail sein, oder gar HTTP ablösen.

Ich kann also auf meinem SIP-Telefon ohne Probleme eine Nachricht von meiner SIP-fähigen Waschmaschine erhalten, die mir mitteilt, dass die Wäsche fertig ist. Sollte mich die Nachricht nicht erreichen, so wird eine SIP-Message mit einer Fehlernummer, ähnlich wie bei HTTP, zurückgesandt. Dabei ist es völlig uninteressant, ob für die Übertragung TCP oder UDP verwendet wird – die Waschmaschine könnte sogar via UDP und Multicast an alle Geräte in einem Hop Entfernung ihre gewünschte Entleerung proklamieren.

Und dieser Punkt macht SIP als Broadcast-Dienst interessant; ob es nun eine einzelne Meldung ist, z.B. ein Alarmsignal an alle Teilnehmer in der Umgebung (wie es im RFC schon beschrieben ist) oder ob an alle SIP-Geräte eine Nachricht gesandt wird, den darin beschriebenen Dienst zu öffnen.

Kommen wir zu den Nachteilen. H.323 muss eine ganze Menge an Paketen hin- und hersenden, um eine Verbindung aufzubauen, was zu einer Pause von mehreren Sekunden führen kann. In der Version 2 wurde daher FastConnect eingeführt, das jedoch nicht immer funktioniert – die Datenübertragung wird schon gestartet, auch wenn noch nicht alle

nötigen Informationen ausgetauscht wurden. Dass die Messages binär versendet werden, liegt daran, dass man sich davon eine Reduzierung des Traffic erhoffte, da Binärnachrichten im allgemeinen kleiner sind als Plaintext-Messages. Der Effekt schmilzt jedoch durch die große Anzahl von versendeten Paketen dahin.

Auch ist es sehr mühselig, bei Problemen im Verbindungsaufbau die erhaltenen Fehlermeldungen erst wieder zu decodieren, was sich wiederum auf die eher negative Bereitschaft, Software für H.323 zu schreiben, auswirkt. Als letzter negativer Punkt ist das komplexe Netzwerk genannt. Im H.323-Dokument wird immer noch von "dummen" Terminals ausgegangen, weswegen die Server die Arbeitstiere sind. Verteilt man nun die Arbeit auf mehrere Server, so müssen diese wieder miteinander verknüpft werden und das Netzwerk wächst gewaltig, bis irgendwann die Leitungen nicht ausreichen und weitere gezogen werden müssen, die auch von Servern "verwaltet" werden usw. Es kann in einem Teufelskreis enden.

Ganz davon abgesehen, dass mehr Server auch mehr Kosten für den Anbieter darstellen, die bei "intelligenten" Endpunkten auf die Nutzer verteilt werden. Bei SIP hat man mit anderen Nachteilen zu kämpfen. Zum einen, dass es das für eine Bandbreiten fressende Audio- oder Videokommunikation nötige Load-Balancing nicht gibt und somit im ungünstigsten Fall die Verbindung getrennt wird anstatt den Clients eine SIP-Nachricht zukommen zu lassen, auf einen anderen (auch schlechteren) Codec umzuschalten. Es wird aber wohl nur eine Frage der Zeit sein, bis es diesen Punkt in SIP auch gibt.

Als letzter genannter Punkt ist ein funktionierendes Netzwerk inklusive DNS erforderlich. SIP-Messages basieren nicht auf IP-Adressen und haben auch keinen Gatekeeper, um Aliase (oder eher Domain-Namen) mit IP-Adressen zu verknüpfen. Es existieren lediglich Proxys, die festhalten, wer derzeit ein SIP-Terminal im Netzwerk angemeldet hat oder eine Weiterleitung speichern.

Das Ende

H.323 ist ein recht ordentlicher Standard – man kann eine Menge an Komponenten und Clients (wie NetMeeting) verwenden und einige funktionierende Netzwerke wurden entwickelt. Man sollte aber immer daran denken, dass es ursprünglich eine Umsetzung vom Telefonnetz auf ein IP-basiertes Netz ist. Aufgrund der Tatsache, dass SIP auf echten Internetapplikationen basiert, kann man es wirklich Internettelefonie nennen. Die aktuelle Entwicklung zeigen, dass dieses Protokoll mehr Freiheiten für die Entwicklung von Features lässt – und das alles mit diesem Gerät, dass ursprünglich Telefon genannt wurde.

Mehr zu VoIP

http://www.packetizer.com/ – das Portal zum Bereich Voice over IP

http://www.openh323.org/ – H.323-Applikationen als OpenSource-Produkte

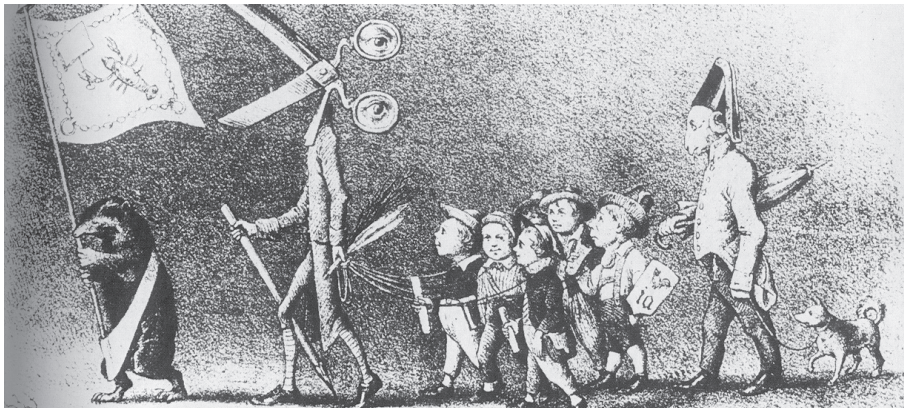
http://www.chaosdorf.de/~pylon/18C3-VoIP.pdf – Folien zu meinem Vortrag über VoIP auf dem 18C3

Literatur

[1] Packetizer (Hrsg.), "H.323 versus SIP: A Comparision", Packetizer Inc., http://www.packetizer.com/iptel/h323_vs_sip/index.html, August 2001.

[2] International Telecommunidcation Union (Hrsg.), "Packet-based multimedia communications systems - ITU-T Recommondation H.323", Telecommunication Standardization Sector of ITU, February 1998.

[3] Handley, et al., "SIP: Session Initiation Protocol", RFC 2543, Internet Engineering Task Force, March 1999.



Willkommen in der kontaktlosen neuen Welt!

von Stefan Krecher

Seit einigen Jahren wird der Einsatz kontaktloser Chipkarten in den unterschiedlichsten Kontexten erprobt (siehe z.B. DS #70, "tick.et: wir wissen, wo sie sind."). Doch jetzt wird es akut: in vielen Universitäten und Hochschulen sind die Karten bereits im Umlauf, bzw. sollen bald eingeführt werden.

Es gab keinen großen Knall und keinen Pressewirbel - die kontaktlosen Chips wurden in vielen Fällen einfach auf dem jeweils neuen Studentenausweisen mit untergebracht. Teilweise gibt es noch keine Anwendungen (angeblich), sondern es wird an den sogenannten "future use" gedacht.

An den betroffenen Unis liefen studentische Organisationen Sturm und versuchten sich zur Wehr zu setzen - datenschutzrechtliche Vorwürfe und Bedenken wurden allerdings von den Behörden abgewiegelt, Kritiker in der lokalen Tagespresse als paranoide Spinner dargestellt. In kleinen und überschaubaren Einrichtungen werden so schleichend Instrumente des Überwachungsstaates eingeführt - mit 30 rebellierenden Studenten wird man dort problemlos fertig.

Resultat ist natürlich auch, dass auf diesem Weg eine breite Akzeptanz für die multifunktionalen Karten geschaffen wird. Wenn das System an den Hochschulen funktioniert, ist der Weg der Chips in andere Lebensbereiche nicht mehr weit.

Schauen wir uns zunächst einmal an, wie diese kontaktlose Technik funktioniert. In vielen Fällen befinden sich auf den neuen Studentenausweisen zwei unabhängige Chips: ein herkömmlicher, kontaktbehafteter Chip (Speicherkarte oder Smartcard) und ein kontaktloser Chip.

Dieser kontaktlose Chip ist in den meisten Fällen ein Mifare-Chip der Firma Philips Semiconductors. Die Kommunikation zwischen Karte und Terminal basiert auf der sogenannten Transpondertechnik, d.h. auf der Karte befinden sich eine Spule und ein Microchip. Das zugehörige Terminal (das Schreib- bzw. Lesegerät) hat ebenfalls eine Spule und erzeugt damit ein Magnetfeld, welches in der Spule der Chipkarte Spannung erzeugt und zur Stromversorgung des Chips beiträgt. Der Datenaustausch wird nun durch Spannungsänderungen realisiert.

Die Reichweite solcher Systeme, die auch RFID (Radio-Frequency Identification) genannt werden (obwohl sie auch RFÜ – Radio-Frequency Überwachung – heissen könnten) ist unterschiedlich. Hersteller von Terminals für die Mifare-Chips sprechen von 10 bis 20 cm, abhängig von der Antennengeometrie. Mit RFID-Systemen sind aber auch größere Entfernungen denkbar, die Norm "Hands Free Integrated Circuit(s) Cards nach ISO/IEC 15 693" befasst sich z.B. mit Karten für größere Reichweiten.

Die hier stark vereinfacht dargestellte Technik wird in [1] und [2] ausführlich beschrieben. Ansonsten ist der Chip je nach Typ (es gibt unterschiedliche Mifare Chips) ISO 7816 und ISO 14443 kompatibel, hat ein EEPROM zum Speichern von Informationen und unterstützt Verschlüsselungs- und Authentifizierungstechniken.

Anwendungsmöglichkeiten

Die Anwendungsbereiche sind vielseitig, die Hochschulen haben schon einiges implementiert bzw. in Aussicht gestellt (siehe Links).

Im einfachsten Fall wird der Chip als Zugangsberechtigung zu Universitätsgebäuden benutzt. Hierbei wird anhand einer Kennung und z.B. der Matrikelnummer geprüft, ob der Karteninhaber berechtigt zum Aufenthalt in bestimmten Räumen ist. Geschickt platzierte Terminals können natürlich aber auch Profile erstellen: welcher Student war wann in welchem Gebäude, in welcher Vorlesung usw.

Der Mifare-Chip eignet sich aber auch als kontaktlose Geldkarte, die an der Uni-Kasse aufgeladen werden kann. So kann dann mit der Karte die Rückmelde-Gebühr bezahlt, Strafe für vergessene Bücher bei der Bib entrichtet und in der Mensa das Essen gekauft werden - vielen Dank für den Fisch.

Die Geldkarte funktioniert dann übrigens ohne PIN, die Unis weisen darauf hin, dass nur kleine Beträge auf die Karte geladen werden sollen.

Weitere Anwendungsmöglichkeiten liegen nahe.

Was sagen die Hochschul-Verwaltungen? Für die Entscheider steht fest: das System ist super-toll, löst viele Probleme. Die Karten haben geringeren Verschleiß und die Terminals entziehen sich gänzlich dem Einfluss der subversiven und destruktiven Studenten, können sogar unterputz, unsichtbar angebracht werden. Im Übrigen deckt sich alles mit der aktuellen (und sicher erst recht mit der zukünftigen) Gesetzeslage und ist mit allen möglichen Datenschutzbeauftragten abgesprochen.

Gerade für die Gebäudesicherung ist das System vor allem für die Sicherheit der weiblichen Studierenden von Interesse. Diese brauchen sich nicht mehr vor Übergriffen der am Cola-Automaten im Rechenzentrum lauernden Perversen zu fürchten...

Das Totschlagargument ist aber: das System darf natürlich nicht zur Schaffung des "Gläsernen Menschen" führen und nur im Rahmen der gesetzlichen Bestimmungen eine Datenverwendung erlauben. In einem Land, in dem ohne gesetzliche Grundlage Soldaten in den Krieg geschickt werden oder ohne gesetzliche Grundlage Überwachungsmaßnahmen durchgeführt werden, ist dieses Argument allerdings nicht sehr beruhigend.

Ausblick

Die kontaktlose Chipkarte ist da, und wird nur schwer aufzuhalten sein. Die Argumente der Unis sind fadenscheinig und polemisierend.

Die Propaganda, die betrieben wird ist angsteinflössend – in der Trierer Tageszeitung z.B. wurden zwar die Bedenken der AStA publiziert, gleichzeitig aber auch drei Studierende vorgezeigt, die die neue Chipkarte "Tunika" eigentlich gar nicht so schlimm finden ("Im Zeitalter des Internet und der Chipkarte ist der Mensch sowieso schon recht durchsichtig. Daher glaube ich nicht, dass durch die neue Chipkarte auf der Tunika der eventuelle Missbrauch verstärkt wird", "Im Großen und Ganzen finde ich die neue Tunika recht gut, man hat durch sie viele Vorteile, ..." und "Ich finde es schade, dass die Rückmeldung jetzt 20 Mark mehr kostet, da ich die zusätzlichen Funktionen der Tunika nicht nutzen werde. Das Gefühl, dass die Universität mich überwachen könnte oder meine Daten weitergeben könnte, habe ich allerdings nicht." siehe [3])

Die Anzahl der Uni's, die solche Systeme einsetzen (wollen) ist kaum noch überschaubar - der Weg zu einer "Bürgerkarte" ist geebnet. Fakt ist, dass diese Systeme sich hervorragend zu Überwachung und Profilerstellung eignen, und natürlich auch noch einiges an Missbrauchspotenzial beeinhalten. Und dann gibt's ja noch die "berechtigten Behörden", die ihren Anspruch auf gespeicherte Daten anmelden werden.

Was kann man tun?

Man sollte sich zunächst mal über das Chipkartensystem der jeweiligen Uni ausgiebig informieren. Welche Informationen werden auf der Karte vorgehalten und wo werden diese Informationen abgefragt, wo werden sie gespeichert? Wo sind die Terminals angebracht, bzw. wo wird geplant solche zu installieren? Gibt es irgendwo verdächtige Umbauarbeiten? Kleine Kästen, die in der Nähe von Türen montiert sind?

Es sollten sowohl Informationsveranstaltungen als auch Boykotte durchgeführt werden. Wer den kontaktlosen Chip auf seiner Karte eindeutig identifizieren kann, sollte sich überlegen, diesen Chip untauglich zu machen, z.B. physisch zu beschädigen.

Studentische Initiativen sollten gegründet werden, Anlaufstellen sind in jedem Fall Organisationen wie Asta, Studentenrat, aber auch Bürgerrechtsorganisation en und natürlich der Chaos Computer Club.

[1] Klaus Finkenzeller: RFID Handbuch, Hanser Verlag

[2] Wolfgang Rankel, Wolfgang Effing: Handbuch der Chipkarten, Hanser Verlag

[3] Trierischer Volksfreund, http://www.intrinet.de/20010712/ts400126.htm

Links

http://www.uni-trier.de/tunika/NeuerStudienausweis_Infos.htm

http://www.uni-leipzig.de/chip2net.htm

http://www.uni-muenster.de/Studierendenschaft/AStA/referate/chipkarte/content.shtml

http://www.fh-worms.de/aktuelles/wolfhart_text.html

http://www.uni-giessen.de/chipkarte/

http://autos.cs.tu-berlin.de/fb13ini/2001_1/chipkarte.html

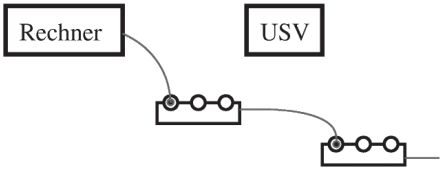
Operation am offenen Herzen

Hubert Feyrer <hubert@feyrer.de>, Marius Strobl <marius@soylent-green.org>

Wie schließt man eine USV im laufenden Betrieb an? Abschalten der Stromversorgung führt zur Unterbrechung des Betriebs. Mit Hilfe einer Unterbrechungsfreien Strom/versorgung (USV) kann dies verhindert werden, doch wie schließt man sie nachträglich an? Der vorliegende Artikel zeigt eine Hardware-Schaltung, die es erlaubt, einen Rechner nachträglich, im laufenden Betrieb und ohne Ausfall, mit einer USV zu versorgen, und dokumentiert die Realisierung der Umsetzung an der Fachhochschule Regensburg.

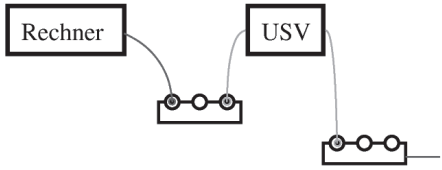
Am Fachbereich der FH Regensburg wird ein Unix-Rechner betrieben, der Studenten via Netzwerk 24x7 zur Verfügung steht. Er wird für Programmierübungen in diversen Vorlesungen sowie für EMail, News und sonstige Online-Kommunikation benutzt. Durch die hohe Verfügbarkeit der Hardware, Software und nicht zuletzt der Stabilität des Betriebssystems (Sun Solaris/x86) hat der Rechner momentan - Stand 18.11.2001 - eine Laufzeit von knapp 600 Tagen ohne Neustart!

Für die frühen Morgenstunden des 19.11.2001 ist eine Abschaltung des Stromnetzes im gesamten Gebäude zwecks Messungen des TÜV anberaumt. Diese Abschaltung ist ein Problem für das Vorhaben, die Stabilität des Rechners anhand einer möglichst großen Uptime zu demonstrieren, da der Rechner ohne Unterbrechungsfreier Stromversorgung (USV) bzw. Notstromaggregat betrieben wird, wie in Bild 1 gezeigt. Ein Herunterfahren/Neustarten des Systems würde die 600 Tage Uptime zerstören, ist also keine Option!



Leihweise ließ sich eine USV auftreiben, so dass der Betrieb des Rechners auch während der Abschaltung des Stromnetzes gesichert werden konnte, wie in Bild 2 gezeigt.

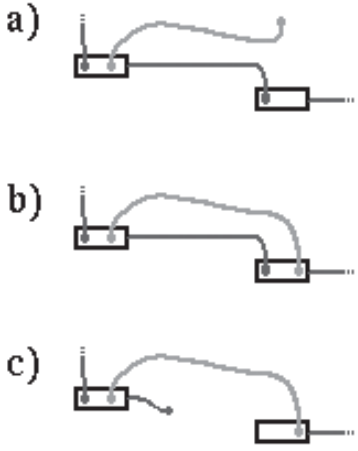
Dass die USV in der Stromversorgung des Rechners zwischengeschaltet werden musste, war ein Problem, da ein Öffnen des Stromkreises ebenfalls gleichbedeutend mit dem Verlust der Laufzeit ist. Es galt eine Lösung zu finden, dies zu verhindern und dennoch die USV anzuschließen!



Idee

Die ersonnene Lösung nutzt die Tatsache aus, dass man verlustfrei eine Verbindung überbrücken kann, wie in Bild 3 gezeigt:

Bild 3a) zeigt die Ausgangslage: Die Verbindung zwischen zwei Mehrfachsteckdosen ist durch das "normale" Kabel (blau) überbrückt. Man kann



Der "Patient" Tabaluga vor der Operation

problemlos ein zweites Kabel (magenta) einstecken, und dann parallel zum ersten schalten, wie in Bild 3b) gezeigt. Anschließend kann man die ursprüngliche Verbindung trennen (Bild 3c).

Über USVs

Bei USVs wird zwischen zwei Typen unterschieden, "offline" und "online". Für das Vorhaben eignen sich Geräte mit "offline" Technologie besser, da man beim Einbau garantiert keine Phasenverschiebung zwischen Netz und USV-Out hat. Im vorliegenden Fall wurde eine "offline" USV vom Typ APC Smart-UPS verwendet.

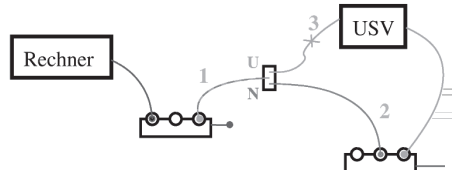
In aller Kürze:

"Online" USV:
Permantente Wandlung, keine Umschaltzeit, bei Netzversorgung wesentlich höhere Verlustleistung, teurer (höhere Qualitätsanforderungen)

"Offline" USV:
Wandlung nur im Bedarfsfall, Umschaltzeit, praktisch keine Verlustleistung bei Netzversorgung, billiger (Wandler-Hardware braucht keiner Dauerbelastung standhalten), keine Phasenverschiebung bei Netzversorgung

Realisierung

Die Realisierung dieser Idee umfasst nicht ein Überbrückungskabel, sondern zwei: Das erste, das die bestehende Verbindung "normal" überbrückt, wie oben gezeigt, und das zweite, das die USV zwischengeschaltet hat. Um später nicht mehrere Verbindungen parallel zu haben und einfach und schnell von einer Überbrückung auf die andere umschalten zu können wurde ein Schalter (2 x UM) benutzt, der jeweils Nulleiter und Phase umschaltet.

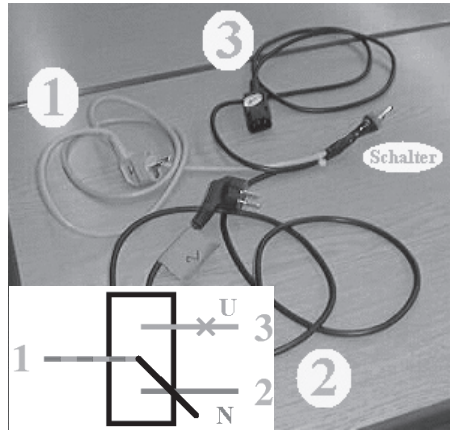


Die drei Schutzleiter wurden direkt miteinander verbunden. Diese beiden Überbrückungen sind im Schaltplan (Bild 4) vereinfacht dargestellt: die magentafarbene Brücke stellt die Verbindung zwischen den beiden Mehrfachsteckleisten ohne USV dar, der Umschalter in der Mitte ist dabei in der Stellung "N" (Netzversorgung). Die Versorgung über die USV ist grün eingezeichnet, die Schalterstellung dazu ist mit "U" (USV) gekennzeichnet. Wichtig dabei ist, dass die USV dabei weiterhin aus dem Netz gespeist wird, und sich automatisch einschaltet, wenn die Spannung am Eingang (grüne Leitung ganz rechts im Bild 4) abfällt.

Bild 4 zeigt den gesamten Aufbau:

Achtung! Die gezeigten Verbindungen laufen allesamt mit 230 Volt Wechselspannung! Neben den üblichen Sicherheitsmaßnahmen ist hier darauf zu achten, dass jede Leitung aus Nulleiter, Phase (-> Strom!) und Schutzleiter besteht. Beim Aufbau der Schaltung, d.h. sowohl beim Einstecken der SchuKo-Stecker in die Steckerleiste als auch beim Einstecken der Kaltgeräte-Anschlüsse an der USV ist darauf zu achten, dass immer Phase auf Phase, und Nulleiter auf Nulleiter gesteckt wird! Kurzschlußgefahr! Neben der Gefahr von Kabelbrand können dabei sowohl Rechner als auch USV Schaden nehmen. Ein Phasenprüfer ist hier hilfreich, im Optimalfall wird ein Multimeter zum Bestimmen der Potentialdifferenz benutzt.

Bild 5 zeigt eine Detailansicht des Umschalters mitsamt der Kabel:



Das grün/magentafarbene Kabel #1 geht hierbei zur linken Verteilerdose, die auch den abzusichernden Rechner speist. Es leitet Strom je nach Schalterstellung aus dem Netz- oder dem USV-Schaltkreis an die linke Steckerleiste. Das magentafarbene Kabel #2 liefert direkt Strom aus der Netzversorgung der rechten Steckerleiste, ohne USV. Die Schalterstellung ist mit "N" bezeichnet. Das dritte, grüne Kabel #3 geht zur USV, und anschließend ebenfalls zur rechten Steckerleiste. Evtl. müssen hier Phase und Nulleiter im Kabel vertauscht werden (vergleichbar einem Crossover-Twisted-Pair Kabel :-), um die Phase des Kabels an den Phasen-Ausgang der USV zu koppeln. (NIEMALS Phase auf Nulleiter - Kurzschluß!). Die rechte Hälfte von Bild 5 zeigt auch die beiden SchuKo-Stecker an Kabel #1 und #2, die jeweils an die Mehrfachsteckdosen angeschlossen werden, sowie den Kaltgerätestecker, der an die USV angeschlossen wird. Das Kaltgerätekabel, das die USV dann an die rechte Steckdose anschließt ist hier nicht gezeigt.

Ablauf Aufbau

Bevor im Folgenden stichpunktartig der zeitliche Ablauf erläutert wird, in dem die einzelnen Kontakte herzustellen bzw. zu lösen sind, folgen hier nochmals die allgemeinen Regeln:

- Immer Phase auf Phase, Nulleiter auf Nulleiter!
- Stecker #1 und #2 nicht vertauschen!
- Die üblichen Vorsichtsmaßnahmen beim Umgang mit Strom beachten!

Hier nun der Ablauf:

1. USV einschalten und Selbsttest abwarten
2. USV-Eingang an rechte Mehrfachdose anschließen
3. Schalter auf "U" stellen
4. Stecker #1 in linke Mehrfachdose einstecken. Vorsicht, es liegt nun Spannung an Kabel(stecker) #3 an!
5. Phase des USV-Ausgangs bestimmen (ist Phase links oder rechts?)
6. Phase von Kabel #3 messen
7. Schalter auf "N" stellen. Vorsicht, es liegt nun Spannung am Kabel(stecker) #2 an!
8. Kabel #3 an USV-Ausgang anschließen, darauf achten dass Phase auf Phase geschlossen wird. Ggf. "gekreuztes" Verlängerungskabel verwenden.

Mit diesem Schritt ist der "grüne" Stromkreis geschlossen, es fließt jedoch momentan noch kein Strom!

9. Phase von Kabel #2 bestimmen
10. Phase der rechten Steckdosenleiste bestimmen
11. Kabel #2 so anschließen, dass die Phasenleitung des Kabels in die Phasen-Buchse der Dose kommt

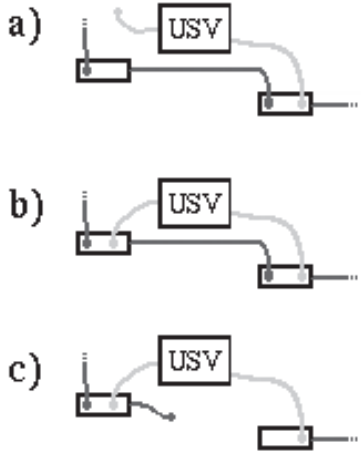
Ab dieser Stelle fließt parallel Strom über den "magentafarbenen" und den ursprünglichen Stromkreis (blau)!

12. Die ursprüngliche Verbindung zwischen den beiden Mehrfachsteckdosen (blau) kann nun entfernt (ausgesteckt) werden. Vorsicht, das Kabel steht unter Strom und muss gegen Berührung gesichert werden, z.B. mit einer "leeren" SchuKo-Buchse!
13. Nun kann der Schalter von "N" auf "U" umgelegt werden, um den Stromfluß vom "magentafarbenen" auf den "grünen" Stromkreis (parallel zum immer noch bestehenden, ursprünglichen blauen Kreis!) umzuschalten.
14. Die Verbindung der beiden Mehrfachsteckdosen läuft nun über die USV, und das gesteckte Ziel ist erreicht

* Ablauf Abbau

Um die gemachten Schritte rückgängig zu machen, ist folgendes Vorgehen anzuwenden:

1. Schalter auf "N" legen
2. Anschluß der "linken" Steckdosenleiste *phasengleich* in "rechte" Steckdosenleiste stecke.
3. Rest in beliebiger Reihenfolge abbauen



Mögliche Optimierung

Der zweite "magentafarbene" Stromkreis ist relativ überflüssig und wurde nur zu Testzwecken eingebaut, und weil durch den Schalter ein schnelleres, rausch/wackelfreies Umschalten möglich ist. Da außerdem damit zu keinem Zeitpunkt der Ausgang der USV mit der Netzversorgung verbunden ist, ist diese Lösung etwas sicherer.

Bei offline USV's, bei denen im Netz-Betrieb der Eingang direkt auf den Ausgang durchgeschleift wird (messen!) ist das Vorhaben auch ohne Schalter realisierbar, was zudem den Vorteil hat, dass die Umschaltzeit nicht vom Computer-Netzteil überbrückt werden muss. Vorsicht: USV's mittlerer bis guter Qualität, z.B. APC Smart-UPS, schalten sich bereits bei Spannungsschwankungen ein, die meistens Netzversorger-bedingten Stromausfällen vorausgehen. Tritt dieser Fall während des Zwischenschaltens der USV ein, so liegt Spannung aus dem Versorgungs-Netz am USV-Ausgang an, was mit hoher Wahrscheinlichkeit zur Zerstörung der USV führt!

Die Möglichkeit, die USV direkt parallel zu schalten (siehe Bild 6) ist für künftige Vorhaben dieser Art zu eruieren. Bei der Durchführung ist darauf zu achten, dass der Eingang der USV (im Bild 6: rechts) zuerst angeschlossen wird, damit die USV hochfahren und den Selbsttest durchführen kann, bevor der Ausgang verbunden wird. (Achtung: Wenn man erst "links" einsteckt liegt nach dem Einstecken "rechts" Netzspannung am Ausgang der USV an, was zu deren Zerstörung führen kann!)

links: Das OP-Team nach erfolgreich verlaufener Operation.

Möglicher Ablauf:

- Eingang der USV mit "rechter" Leiste verbinden
- USV einschalten, Selbsttest abwarten
- Ausgang der USV phasengleich mit "linker" Leiste verbinden
- "Linke" Leiste aus "rechter" Leiste ausstecken
- Stecker der "linken" Leiste vor Berührung der Kontakte sichern!

Disclaimer

Wer nicht *genau* weiss, was er beim Experimentieren mit Strom macht, sollte besser die Finger davon lassen (oder einen Experten hinzuziehen)!

Die Folgen können von Stromausfall mit verbundener Downtime und Betriebsausfall über Hardware-Schäden bis hin zu tödlichen Stromschlägen führen. You have been warned!

Weder der Autor dieses Artikels, noch die Datenschleuder, noch sonst irgend jemand übernehmen irgendeine Haftung für die gemachten Angaben!

Links

Hier zum Abschluß noch ein paar interessante Links zum Thema USVs:

- *http://www.zdnet.de/produkte/artikel/hwmisc/200108/usv02_01-wc.html*
- *http://eces.de/usv.htm*
- *http://www.jentech.de/en/english/produkte/liebert/infopage.html*

Robert Anton Wilson über die Risiken des Kokainmissbrauchs:

"Zwei bekannte politische Führer hatten angeblich diese ruchlose Gewohnheit.

Beide kamen aufgrund zweifelhafter Wahlen, durch undemokratische, irreguläre Methoden, an die Macht

Beide Nationen erlebten unmittelbar Anschläge auf berühmte öffentliche Gebäude.

Beide beschuldigten eine ethnische Minderheit bevor die Ermittlungen Beweise erbracht hatten.

Beide führten "Hexenjagden" gegen die beschuldigte Minderheit durch.

Beide setzten bürgerliche Freiheiten "zeitweise" aus.

Beide stellen die Bevölkerung unter Beobachtung.

Beide unterhielten verborgene, geheime Regierungen.

Beide erklärten nahezu der gesamten Welt den Krieg.

Einer hatte einen lustigen Schnauzbart. Wie hieß der andere?"

Quelle: http://www.broeckers.com/Interview-RAW.html bzw. *http://www.telepolis.de/deutsch/special/wtc/12696/1.html*

Reverse-Engineering für Ortsfremde

von Erdgeist

Seit einer Woche nun bin ich stolzer Besitzer einer Telefonbuch CD. Genau, die Telefonbuch CD für ganz Deutschland. Von der Telekom. Mit Routing. Ich wollte die Telefonnummer meiner Oma rausfinden und mir ne Wegbeschreibung zu ihr ausgeben lassen. Und nun sitz ich da vor meiner MicroVax II und, was soll ich sagen? Geht nicht.

Is blöd, denk ich mir und guck mir das an und siehe da: Eine Windows-.exe und ein linux-install.sh. Die linux-binaries sind in einem seltsamen Format und brauchen krumme SuSE-libraries. Nun bin ich erstmal verzweifelt. Oma ist bestimmt traurig. Ich ls'e mal ein wenig auf den CDs rum und: da liegt auf der 2. CD unter atb/dat doch glatt eine teiln.dat rum. Hört sich spannend an. Vielleicht bekomm' ich die Nummer nun doch noch vor Omas Geburtstag raus. Aber irgendwie mag aus der Datei nicht so richtig Klartext herausfallen und ich zerschiesse mir erst einmal mein Terminal.

Hexdump ist ein besserer Freund, aber an das Telefonbuch erinnert mich der Datensalat immer noch nicht. Und 'grep Oma teiln.dat' findet auch nichts. Da liegen zum Glück aber noch andere Dateien herum, die heissen so vorn.dat. Ich hoffe, dass die mir vielleicht weiterhelfen. In Gedanken seh ich mich nun fast schon wieder an der Kaffeetafel mit dem besten Zupfkuchen der Welt. So richtig nach Vornamen sieht auch das nicht aus, aber der String "-lh5-" erinnert mich an was. Der steht da nämlich genau an Byte 2 und dann später wieder und, wer hätte es gedacht, ziemlich häufig, immer mal wieder in der Datei und kurz dahinter BLK00xxx.DAT.

"Abgefahren", denk ich bei mir, krame die Lha-sourcen hervor, compile die und "ei der Daus" – wie meine Oma jetzt sagen würde – fällt da eine ziemlich lesbare blk00000.dat raus, mit so ein paar Vornamen drin, obgleich ich zweimal hingucken muss, so ganz richtig gewöhnlich ist Aafje und Aage nicht, aber einen Achibert kenn ich, so heisst Opa. Prima. Lha scheint der richtige Weg zu sein. Ich mach mich kurz los, um schonmal Backzutaten für den Geburtstagskuchen und eine Flasche Wein zu kaufen. Wär doch gelacht, wenn ich nicht auch noch Omas Nummer fände.

Die anderen Dateien, wie ortstr.dat und messe.dat sind auch alle ge-lha-t, aber bringen mich nicht weiter. Es muss die teiln.dat sein. Und da springt es mich förmlich an: an Byte 2 und an Byte 6, da wo in den anderen Dateien die '-' von "-lh5-" stehen, stehen in der teiln.dat 0x1d's, und dahinter, wo die *most significant bytes* der *compressed* und *uncompressed filesize* (siehe Grafik Lha-Header-Format) stehen, also meistens Null, stehn auch zweimal 0x30. Und wenn ich noch weiter in der Datei rumsuche, stehen an der Stelle vom zweiten Byte der sizes ziemlich häufig 0xbc's. Die können doch nicht beide für ein 0x00 stehen? Oder doch?

Ich kann mich inzwischen kaum noch konzentrieren, weil ich nur noch an eine grosse Tafel mit Kohlrouladen denken kann, aber ich zwinge mich, weiterzusuchen. Wenn Bytes 2 bis 6 wirklich "-lh5-" repräsentieren sollen, und die 4 Bytes danach die compressed file size würde das folgendes bedeuten:

```
???? ???? 0x2d 0x6c 0x68 0x35 0x2d ???? ????
0x00 0x00 0x9c 0xfb 0x1d 0x6d 0xef 0x89 0x1d
0x38 0xea 0xbc 0x30
```

macht nachm xor:

```
???? ???? 0x30 0x01 0x87
0xbc 0x30 ???? ???? 0xbc 0x30
```

Boah, denk ich, 3 x 0x30 im Abstand von 4 Bytes, und 2 x 0xbc im Abstand von 4 Bytes. Ich nehm mal an, dass 0x87 0xbc 0x30 0x01 ein magisches Muster sein muss und bekomme nachfolgende Tabelle:

Header size	0x1b = 27	hört sich ganz gut an, bedeutet, dass die Länge des Dateinamens 5 sein sollte, mal schaun
Checksum	0xd9	nachher mal die checksum vom header bilden, das ist einfach nur Summe der header bytes modulo 256
Method	"-lh5-"	klar, davon sind wir ja ausgegangen
Compressed size	0x0000 0x6d39	kann man ja mal im file seeken, ob nach 0x6d39 + 0x1b + 2 Bytes ein neuer Header kommt
Uncompressed size	0x0002 0x09d6	kann hinkommen
Timestamp	0x0000 0x2821	eigentlich egal
File Attr	0x20	Ooch egal
Header Lev	0x00	das ist gut, sonst würde die Headersize nicht hinkommen, 0x01 würde "header extension" bedeuten
File Name Length	0x05	ahhh, ein Zeichen von sanity
File Name	"R.FRF"	naja, zumindest syntaktisch korrekt
Data checksum	0x9ff2	gleich mal den CRC der Daten vergleichen.

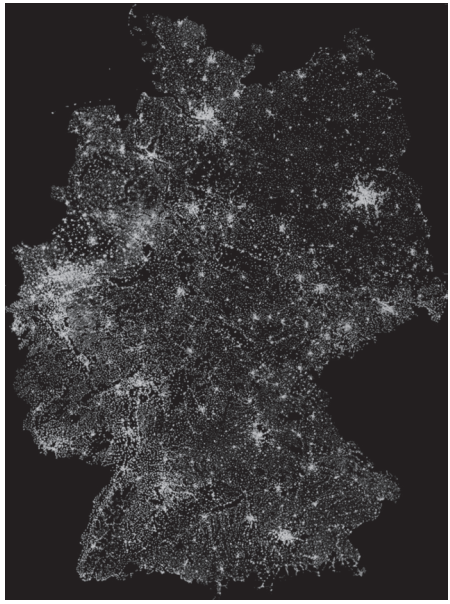
Entmutigend sah das nicht aus. Das Problem ist nur, dass die Checksumme der compressed data noch stimmt, wenn ich die Daten nicht xor-e, danach nicht mehr. Nunja, 29 Bytes zu xoren, wäre ja blöd, wegen ist nicht durch 4 teilbar, also wohl eher 32 und siehe da, da plumpst mir doch glatt eine Datei f.frf vor die Füsse, in der so Zeug wie "Dipl. Ing" und "Flensburg" drin steht. Nur nicht Oma :(. Alle Blöcke von Hand zu entpacken ist auch zu mühsam, also mal schnell ein kleines Programm gehackt. Lieberweise enthält atb/idx/teiln.idx schon vernünftige Indizes auf die Blöcke, also seeken, 32 bytes laden, mantra xoren, dem filename eine fortlaufende Nummer abgeben, damit sich nicht die Blöcke gegenseitig überschreiben, checksum neu berechnen und an Byte 1 schreiben, 32 Byte ausgeben, <compressed size> Bytes aus teiln.dat ausgeben, file zu, neues File auf... macht 35616 Dateien. Boah. Und irgendwo da drinne Oma.

Nach einigem Kramen in meinen Shell-script Kenntnissen würg ich noch "for a in *; do lha -x $a; done" hervor und bekomme ein Muster:

```
00000 - Melted : oooooooooooooooooo
00001 - Melted : ooooo
00002 - Melted : ooo
00003 - Melted : oooooooooooooooooo
00004 - Melted : ooooo
00005 - Melted : ooo
```

und so weiter. Und beim Nachgucken: 00000 kannte ich ja schon, 00001 hat lauter Nachnamen, 00002 lauter Vornamen. und zwar genau 3000 Stück, alle beide. Also nehm ich mal an, dass das bei Datei 00000 auch so aussieht. Dem Anschein nach stehn da "Anrede, Namenszusätze (z.B. :'u. Sohn'), Ortsnamenszusätze, eine Hexadezimalzahl mit Semikolon und einem Grossbuchstaben... mal sehn, eine Hausnummer, eine Postleitzahl, eine Städtebezeichnung, eine Vorwahl, eine Telefonnummer, eine E-Mail-Adresse und eine URL. Null-terminiert. Und hinternander. Naja Strings in Arrays lesen und wieder auszugeben ist Handwerk, nur dass die Strassen fehlen, ist blöd, weil es gibt ja viele Omas und sogar in dem Dorf, wo Oma wohnt.

Aber wir haben ja noch eine mystische Hex-Zahl. Mit Komma und Grossbuchstaben. Und eine Datei namens strassen.dat. Mit ganz vielen lha- gepackten Strassennamen. Null-terminiert. Und hintereinander. Naja, in Blöcken hinternander. Diesmal ohne xoren. Also c-source umhacken. Diesmal ist der Header auch grösser, weil der Filename ja BLK00xxx.DAT ist... nerv, aber bald hab ich eine Strassenliste zusammen. Und nun sollte doch nicht etwa gar die Hex-Zahl ein Index in die Strassennamentabelle sein!? Ich guck bei meiner Telefonnummer nach, weil die weiss ich ja und nehm den Index und guck nach und da steht sie. Meine Strasse.Wieder rumschnippeln und schwupps, produzier ich Daten. Aber ganz viele, um 2.3GB und grep braucht auch ganz lange, aber endlich! Omas Nummer. Und was sie sich freut! Und dass das Routing nicht geht ist auch egal, weil Oma mir bestimmt 4 mal erzählt, wie ich zu ihr finde. Und gleich morgen tausche ich die CD im Laden um und kauf mir was von O'Reillys. Für die lange Fahrt.



Die Karte zur CD – die Adresskoordinaten geolokal gemapped; für jede Adresse wurde der Helligkeitswert des zugehörigen Pixels erhöht.

Ex Machina – Are friends electric?

Von Nika Bertram

So ähnlich muss es in vergangenen Jahrhunderten auch bei Automata-Ausstellungen zugegangen sein: die Begegnung zwischen Mensch und Maschine, mit elektronischen Hilfsgeistern für alle Lebenslagen. Der Robo, dein Freund und Helfer. Bis zum 14. April 2002 zeigte das Kölner Museum für Angewandte Kunst die Geschichte und Zukunft der Roboter in familienfreundlichem Sonntagsnachmittags-Gewand.

Doch wo Vaucansons berühmte "Mechanische Ente" bereits im 18. Jahrhundert schwimmen, quaken, mit den Flügeln schlagen, Essen verschlingen und damit das Publikum narren konnte, wirken die Exponate dieser Ausstellung seltsam leblos. Vielleicht, weil den meisten von ihnen, nach 2-monatigem Ausstellungsbetrieb, die Batterien ausgegangen sind und sie nur noch saft- und kraftlos, wie ausgemusterte Krieger, herumstehen. Das ist schade. Wie es überhaupt schade ist, dass einige Stücke es nicht hierhin geschafft haben. Wie z.B. Kismet, der grade in Paderborn gastiert, und ein heimlicher Favorit besonders des weiblichen Publikums zu sein scheint - wie die drei netten englisch-sprachigen Ladies beweisen, die neben mir schon bei einem Hochglanz-Foto dieses KI-Gremlins in Entzücken ausbrechen. Oder ASIMO, der, so die Veranstalter, leider immer noch beim Zoll festhängt. Na ja, dafür sind AIBO und PaReRo gekommen.

Es ist ein bisschen wie im Zoo, oder einem Kuriositäten-Kabinett. So bleibt angesichts der mangelnden Bewegungsfreude der Maschinen und der etwas dürftigen technischen Infos in Katalog wie Ausstellungsführer den Besuchern gar nichts übrig als zu menscheln, und Erwartungen auf die Kisten zu übertragen, die sie gefälligst zu erfüllen haben. Der emsige Mähroboter RL 800 begrüßt dann auch die Besucher, in dem er beruhigend surrend den Rasen umzuwuseln verspricht.

Der gar nicht putzige Oktoputz hängt jedoch einsatzverweigernd an der Wand herum, Pinochio, der kleine Versuchshumanoide vom Fraunhofer-Institut AiS, gönnt sich eine kleine Verschnaufpause auf seiner mit Spielklötzchen an den Seilen verzierten Präsentationsplattform, und die RoboCupPlayers haben auch gerade Halbzeitpause. Etwas gruseliger wird's dann schon bei CASPAR, dem OP-Robo. So präzise seine lange, feine Spitze auch fräsen mag, man möchte so etwas eigentlich nicht am eigenen Körper herumfummeln lassen.

Den hektischen, etwas neurotisch wirkenden ULIXES allerdings auch nicht. Aber der ist ja nur ein Würstchensortierer. Und wenigstens bereit dazu, sich austesten zu lassen. Legt man ihm die Gummi-Würstchen grade aufs Band, sortiert er sie zackig nach Krümmung, liegen sie übereinander, schmollt er und wibbelt aufgeregt hin und her, wie ein Boxer vor dem nächsten Schlag.

Der Sony-Vierbeiner AIBO (Artificial Intelligence roBOt) ist autonom und lernfähig, besitzt Berührungs-sensoren, Mikrofone, eine Kamera, Gleichgewichtssinn, und eine eigene Spracherkennungssoftware, mit der seine Umgebung analysieren und auf sie mit sechs verschiedenen "Emotionen" reagieren kann. Seine Reaktionen lassen sich durch positive Verstärkung sowie selbst geschriebene Programme steuern, was ihm auch schon eine eigene Liga im RoboCup eingebracht hat. Natürlich gibt es auch einen Basketball-spielenden DUNKOBOT von LEGO Mindstorms zu sehen, ebenso wie ein Industrieroboter-Set von Fischertechnik. In der gleichen Ecke stehen auch die Modelle der neuesten persönlichen Service-Robos, der R100 und sein Nachfolger PaPeRo (Partnertyp Personal Robot). Beide haben neben ihrem R2D2-meets-Playmobil-Look und dem damit verbundenen unschlagbaren Niedlichkeitsvorteil aber mehr zu bieten als meep-meep. Ich zitiere mal aus dem Ausstellungsheft: "Er rollt durch seine Umgebung und sucht menschliche Gesellschaft. Findet er keine, so macht er ein "Schläfchen" und wartet, dass ihn jemand ruft. Erhält der PaPeRo eine Nachricht, die er einer Person ausliefern soll, so beginnt er, diese Person zu suchen. Er erkennt sie anhand ihres Gesichtes und ruft ihren Namen." ... Und jetzt alle: "Süüüüüß!" Oder hier: "Ist R100 allein, dann überwacht er seine Umgebung und wenn er auf etwas ungewöhnliches wie einen Einbrecher trifft, dann nimmt er ihn auf

Video auf und benachrichtigt seinen Besitzer über Internet." Na, das möcht' ich noch sehen.

Richtig knorke wäre es natürlich gewesen, alle diese zuletzt genannten Robos mal live in action sehen zu können, aber das blieb ein Traum. Ein Besucher versuchte PaPeRos Köpfchen (zugegeben, eher unsanft) zu verdrehen ... und wurde sofort zurecht gewiesen. Ok, dreimal pro Tag werden auch zwei Exponate extra vorgeführt, aber in den zwei Stunden, in denen wir dort waren, waren dies nur zwei eher unspektakuläre Geräte.

Dass permanente Hilfsbereitschaft auch nerven kann, wissen wir ja spätestens seit den sprechenden Türen von Douglas Adams oder dem Nervbalg in "A.I.". Richtig böse wird's allerdings, wenn diese Robo-Viecher auch noch anfangen, Johanna von Koczian's Putzschlager "Das bisschen Haushalt..." zu schmettern, während sie den Boden wischen. So geschehen bei dem einen live vorgeführten Kandidaten, dem Reinigungs-Robo ST82 R VARIOTECH. "Treten Sie bitte zurück, ich beginne zu reinigen," kündigt das Teil sein Vorhaben an. Und schon springt man zur Seite. Stellt sich ihm etwas in den Weg, ertönt ein penetrant servil-freundliches "Entschuldigen Sie, ich möchte hier reinigen." Tritt man immer noch nicht zur Seite, wischt es schließlich um einen herum, wie dereinst Mama, und irgendwie wünscht man sich dann, es möge doch auch einmal ein "Geh mir endlich aus dem Weg, Du ...!" brüllen, aber nein, zu menschlich sollen die Dinger ja auch nicht werden.

Das zweite Vorführgerät ist TEODOR, ein Minenentschärfungs-Robo, der seine Bewegungen sehr bedächtig, fast schon elegant tänzerisch, darbietet. Oder wie es ein kleiner Junge ausdrückte: "Was soll denn das? Ist das alles?"

Nun ja, das war schon die Haupthalle. Wir suchen immer noch Kraftwerk. Die sollen hier auch irgendwo herumstehen, als Update, im Expo-Remix. Im zweiten Raum noch ein paar Highlights: der Stanford-Arm, noch mehr spinnenartige, hexapodische, Knickarm- oder Lauf-Robos, Elsie & Elmer, die berühmten Schildkröten. Und auch hier gruselt's wieder leicht: Wabot-1, der erste humanoide Roboter von 1973, also quasi Benders Vorfahre. Das Kerlchen schaffte immerhin einen Schritt in 45 Sekunden. Daneben ein künstlicher Arm für Behinderte. Auch nicht richtig vertrauenserweckend.

Wo sind bloß Kraftwerk? Wir suchen den dritten Raum, verlaufen uns, landen beinahe in der Abteilung "Handwerkskunst im Mittelalter." Nein, hier nicht. Ah, noch 'ne Tür mit Licht. Und es wird dunkel. Genau. Und da stehen sie auch schon, als Leihgabe aus Düsseldorf (ausgerechnet...), neongrün gestreift in schwarzen Boxen, darunter je ein Monitor mit ... nun ja, bisschen Sound dazu wär auch nicht schlecht gewesen. Aber gegenüber, im Kinosaal, läuft ja ein Video. Irgend ein Streifen, der zeigt, wie praktisch Robos sind, die auf Firmenklos neues Klopapier oder Pizzas bringen können. Aha. Wir haben leider nicht mehr die Zeit, auf einen neuen Film oder gar Sounds von Kraftwerk zu warten, und werfen noch einen Blick auf einen Industrie-Robo, der immer wieder das Wort "ART" zusammenlegt, alles wegschüttet, neurotisch wibbelt, und von vorne anfängt. Wie tiefsinnig. Die elektrischen Fische im Aquarium sind auch entzückend, die Quallen allerdings schon tot - das heißt, hoppla, ihre Batterien wohl einfach nur genauso alle wie die von RHINO, dem Museums-Robo, der abgeschlafft mit seinen vollen, künstlichen Lippen in der Ecke herumsteht. Auch schade, wie so vieles bei dieser Ausstellung, die sicherlich gut gemeint war.

Werbeplakat einer Security-Firma. Photographiert von Tina auf dem Flughafen Zürich

Webseiten hinter Glas

von Tom Lazar

Am 23.5.2002 ;-) eröffnete in Frankfurt a. M. die Ausstellung "I Love you" mit dem griffig-schmissigen Untertitel "Computer, Viren, Hacker, Kultur". Die Tatsache, dass selbige nicht in irgendeiner Hinterhof-Galerie stattfindet sondern im mak (Museum für angewandte Kunst) am Museumsufer macht die Sache gleich doppelt interessant: so kann der geneigte Hacker nicht nur (möglicherweise) neue Zusammenhänge zwischen Kunst- und Hackerwelt erfahren, sondern auch, welches Hackerbild in der Kunstszene vermittelt wird.

Der erste Eindruck ist vielversprechend: grosses helles Gebäude, freundliches hilfsbereites Personal, schon in der Eingangshalle sind überall Surfstationen von Sun zu sehen. "Zur Virus-Ausstellung? Zweiter Stock." Vorbei an Möbel-Exponaten und Design-Objekten geht es hinauf "zu den Computern". Begrüßt werden wir von einer großen Texttafel, die wir aber angesichts der dahinterliegenden einladend blinkenden und fiependen Hardware erstmal links liegen lassen.

Der anfänglichen Begeisterung folgte aber baldige Ernüchterung als wir herausfinden, dass die Ausstellung, sagen wir mal "recht übersichtlich" ist. Der Großteil der Exponate gehört zur ständigen Ausstellung. Zwei iMacs mit Ascii-Webcam. Ein Sun-Server in einer Vitrine. Spielkonsolen aus den Achtzigern mit zwei ungefähr achtjährigen Jungs davor, die zwar eifrig bei der Sache, ob der antiquierten Grafik aber doch irgendwie befremdet sind.

Gegenüber steht eine weitere Batterie von Sun-Stations mit TFT-Displays und laden zum Surfen ein – im Gegensatz zu den im Foyer besitzen sie nämlich eine Tastatur zur Eingabe von URLs. Auch hier ein paar Kids, die sich virtuos durchs weltweite Netz klicken, hin und wieder aber klammheimlich leicht verwirrte Blicke austauschen, weil eben doch alles ein wenig anders ausschaut wie bei Papas Windowsrechner zuhause.

Einmal um die Ecke gebogen wo Knautschsessel vor zwei Videoplayern mit Kopfhörern zum Chillen einladen, vorbei an einem Windows XP Rechner auf dem eine Installation von Anti-Mafia[1] läuft, kommen wir dann zum Herzstück der Ausstellung: eine Reihe von Printouts mit "cyberpoetry" gegenüber einer Handvoll von Infokiosken zum Thema Auswirkungen von Virenbefall. Es gibt Videos mit simulierten Virenaktionen (Payloads).

Und dann der Höhepunkt: ein Windowsrechner mit einer CD randvoll mit 6.000 echten Viren, fein säuberlich in Unterordnern sortiert, komplett mit README.TXT und ausführbarer Datei. Ein kleines Schild weist darauf hin, dass bei akutem Virenbefall das Personal verständigt werden kann, welches dann baldmöglichst ein frisches System installieren würde. Zum Zeitpunkt unseres Besuches zierte den Bildschirm lediglich ein Bluescreen.

Wir biegen um eine weitere Ecke und stellen fest, dass wir uns wieder am Eingang befinden. Nach kurzem Innehalten wird uns amüsiert bewußt, dass sämtliche Rechner von Apple oder Sun sind und die einzigen beiden Windowsrechner lediglich zur Demonstration von Viren bzw. Anti-Mafia (einem gnutella-basiertem Windows-only P2P-Programm) dienen.

Die Ausstellung hinterläßt gemischte Eindrücke. Einerseits ist sie professionell in Szene gesetzt: das Ambiente ist hervorragend. Der geringe Umfang wird – zumindest teilweise – durch die ergänzende ständige Ausstellung kompensiert (auch die anderen Stockwerke des mak haben durchaus Sehenswertes zu bieten – der Eintritt zur "I love you"-Ausstellung bietet auch Zugang zu den übrigen Bereichen. Auf Nachfrage wird zum selben Preis sogar eine Monatskarte gewährt.)

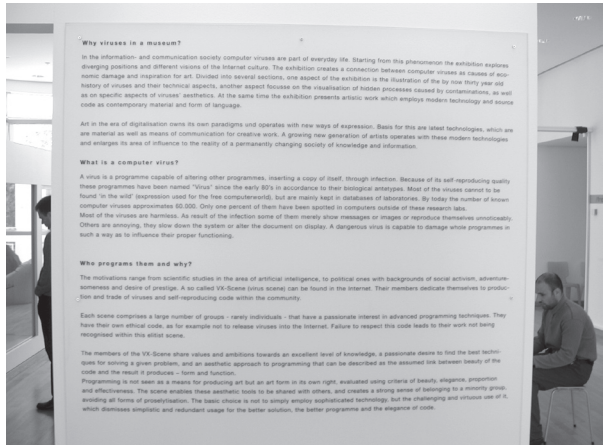
Trotzdem bleibt ein schaler Nachgeschmack. Man wird den Eindruck nicht los, dass man sich mit den Füßen durch eine kleine, feine Website geklickt hat. Das hängt bestimmt mit dem abstrakten Thema der Ausstellung zusammen: schließlich hat auch die Filmindustrie ihre liebe Not mit der Visualisierung von Computerviren (Independance Day, The Matrix etc.) Schade ist es aber allemal.

Die Ausstellung [2] läuft noch bis zum 13. Juni im Museum für Angewandte Kunst [3], Schaumainkai 17 in Frankfurt, jeweils Dienstag bis Sonntag von 10 bis 20 Uhr zu sehen. Eintrittspreis 5 Euro.

[1] *http://epidemic.ws/antimafia/*

[2] *http://www.digitalcraft.org/index.php?artikel_id=237*

[3] *http://www.mak.frankfurt.de/*



Die Höhepunkte der Ausstellung: links oben ein vireninfizierter Windowsrechner. Mit Bluescreen. Wow… oben rechts: der vielbeschworene *Content*, mehrere Texttafeln "Bleiwüste" mit sinnigen Allgemeinplätzen wie z.b. "What is a computer virus? A virus is a programme capable of altering other programmes, inserting a copy of itself, through infection." Soso…

Ansonsten gab es noch viel Hardware der Firmen Sun und Apple zu bewundern, teils – irgendwie absurd – in Vitrinen (s. links und links unten) oder als Surfterminals (links im Hintergrund). Der Kulturteil wurde mit Ausdrucken von perl-lyrik und obfuscated-code sowie einem Zitat des Dalai Lama abgefeiert. Naja…

Vorratsspeicherung von Telekommunikationsdaten

von Sebastian

Ende Mai gab es gleich zwei Entscheidungen zum Thema Vorratsspeicherung von Telekommunikationsdaten. Am 29./30.05.02 verabschiedete zum einen das EU-Parlament eine neue Richtlinie zum Datenschutz, die die Vorratsspeicherung explizit zuläßt [1]. Zum anderen verabschiedete der Bundesrat am 31.05.2002 einen noch vom Bundestag zu verhandelnden Gesetzesentwurf, der Mindestspeicherfristen für Telekommunikationsdaten in Deutschland vorsieht [2].

Hintergrund dieser beiden Entscheidungen ist der Wunsch der Strafverfolgungs- und Sicherheitsbehörden, im Falle eines Falles auf lange in der Vergangenheit zurückliegende Verbindungsdaten zurückgreifen zu können. Zur Zeit werden in Deutschland die Verbindungsdaten spätestens 80 Tage nach Rechnungserstellung wieder gelöscht. Geht man von einem monatlichen Abrechnungszeitraum aus, so sind damit in der Regel die Gesprächsdaten des letzten Vierteljahres vollständig verfügbar. Allerdings liegt der Grund der Erhebung und Speicherung der Verbindungsdaten in der Rechnungserstellung bzw. in der technischen Sicherstellung des Betriebs. Anderweitig dürfen nach den derzeit geltenden Datenschutzgesetzen keine personenbezogenen Daten protokolliert werden.

Bei Pauschaltarifen, insbesondere bei den Internet-Flatrates, werden die einzelnen Verbindungen nicht berechnet, es besteht daher auch keine Notwendigkeit, sie zu erheben oder zu speichern, auch wenn dies in der Praxis oft dennoch passiert. Die Pauschaltarife stellen somit ein Problem für die Strafverfolgungsbehörden dar; denn ohne Verbindungsdaten läßt sich nachträglich kaum überprüfen, ob ein Anschlußinhaber zu einem gewissen Zeitpunkt online war und ob eine Verbindung zu dem fraglichen Angebot bestand. Aber selbst bei einer Erhebung der Daten reiche der Zeitraum von einem Vierteljahr oftmals nicht aus, da manche Delikte wie Kreditkartenbetrug erst sehr spät entdeckt würden und es bereits Monate dauern könne, bis der Fall den geeigneten Stellen übergeben werde. Auch im Zuge internationaler Ermittlungen sei man auf Speicherfristen von einem Jahr angewiesen, um erfolgversprechend zu ermitteln [3].

Nach dem Wunsch der Strafverfolgungs- und Sicherheitsbehörden sollen also sämtliche Telekommunikationsdaten erhoben und für eine gewisse Zeit gespeichert werden. Im Gespräch sind derzeit Mindestspeicherfristen von sechs Monaten bis zu zwei Jahren. Eine solche Maßnahme würde alle Nutzer von Telekommunikationsdienstleistungen jeglicher Art betreffen. Datenschützer warnen vor einer solchen Pauschalspeicherung: Sie stelle einen erheblichen Eingriff in die Persönlichkeitsrechte, das Grundrecht auf informationelle Selbstbestimmung und die Meinungsfreiheit dar. Außerdem werde mit der Vorratsdatenspeicherung der Grundsatz der Unschuldsvermutung de-facto abgeschafft. Schließlich seien von der Vorratsspeicherung nicht nur auffällig gewordene Personen auf individuelle Anordnung einer Behörde hin betroffen, sondern in erster Linie gesetzestreue Bürger. In einer Presseerklärung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein wird ein solches Vorgehen mit einer Vorratsspeicherung von Einkaufsdaten verglichen: „Stellen Sie sich vor, Sie würden beim Betreten jedes Einkaufszentrums registriert und es würde genau notiert, was Sie dort ansehen, wie lange Sie ein Buch oder irgendeine Ware in der Hand halten, welche Zeitschriften Sie kaufen, von welchem Laden Sie in welches Geschäft gehen und für welche Produkte Sie sich interessieren, usw." [4] Der Kasseler Rechtsprofessor Alexander Roßnagel sieht in der Vorratsdatenspeicherung sogar einen Verstoß gegen die Verfassung: „Kommunikationsinfrastrukturen vorrangig nach Überwachungsinteressen zu gestalten, ist nicht freiheitsverträglich. Vielmehr muss gelten, dass die Überwachungsbehörden im begründeten Ausnahmefall auf die Daten zugreifen können, die vorhanden sind. Eine Vorratsspeicherung aller Daten ohne eine solche Begründung ist nach dem Volkszählungsurteil des Bundesverfassungsgerichts verfassungswidrig." [5] Neben der Rechtsproblematik stellt die Erhebung und Speicherung der Daten für den Betroffenen auch ein Risiko dar. Überall, wo Daten erhoben werden, müssen sie besonders gegen unbefugten Zugriff geschützt werden. Dies läßt sich aber nicht sicherstellen. Auch steht zu befürchten,

daß die Daten viel länger als vorgesehen aufbewahrt werden, z.B. in Form von Backups.

Trotz dieser Bedenken fielen die Entscheidungen des EU-Parlaments und des Bundesrats zugunsten der Vorratsdatenspeicherung in der EU und Deutschland aus. In Artikel 15 der vom Europaparlament verabschiedeten Richtlinie [1] heißt es: „Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel [...] dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel [...] für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit oder die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch entsprechende Rechtsvorschriften vorsehen, dass die Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. [...]“

Der Hintergrund der Öffnung der Datenschutzrichtlinie für die Vorratsdatenspeicherung wird in einer vertraulichen Agenda eines Treffens von Experten im Rahmen von Europol deutlich, die von Marco Cappato, Abgeordnetem des Europaparlaments, veröffentlicht wurde [6]. Aus dem Europol-Dokument geht hervor, daß im Hintergrund bereits an einer EU-weiten Einführung der Vorratsspeicherung von Telekommunikationsdaten gearbeitet wird. So sollte bei dem Treffen ein gemeinsamer Standpunkt der EU-Strafverfolger zur Vorratsdatenspeicherung diskutiert werden. Eine umfangreiche Liste der zur erhebenden und zu sichernden Daten wurde ebenfalls beigefügt. Für das Internet werden die Bereiche Zugangsanbieter (TACACS+ und RADIUS-Logs, Rufnummer, Zahl der übertragenen und empfangenen Bytes, Kreditkarten- und Kontodaten des Kunden), E-Mail-Dienstleister (SMTP-, POP-, IMAP-Logs), Upload- und Download-Server (FTP-Logs), Webserver (HTTP-Logs, auch Änderungen der Webseiten durch den Kunden), Usenet (NNTP-Logs) und Chat-Server (IRC-Logs, Nicknames, Kontodaten der Kunden) abgedeckt. Noch länger ist die Liste der zu erfassenden Daten für Telefondienst-Anbieter: Unter anderem werden die kompletten Adress- und Geburtsdaten der Kunden, die gewählten und empfangenen Rufnummern (unabhängig vom Zustandekommen einer Verbindung), Dauer, Rufweiterleitungen, Art der Kommunikation und Kontodaten sowie Zahlungsweisen gefordert. Bei Mobilfunkkunden kommen geographische Angaben und WAP- und SMS-Dienste hinzu. Bei GPRS und UMTS gelten zusätzlich die Bestimmungen für Internet-Anbieter.

Noch weiter geht der am 31.05.2002 im Bundesrat mit der Mehrheit der Unions-geführten Länder beschlossene Gesetzesentwurf „zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen“ [2]. Neben einer Zulassung des Einsatzes von sogenannten IMSI-Catchern sieht der Gesetzesentwurf auch die Einführung der Vorratsdatenspeicherung in Deutschland vor. Dabei sollen die Daten nicht nur zur Strafverfolgung, sondern für die Erfüllung sämtlicher Aufgaben von Polizei, Verfassungsschutz, Bundesnachrichtendienst, Militärischem Abschirmdienst und Zollkriminalamt genutzt werden können [4]. Wie lange die Daten gespeichert werden müssen und wie darauf zugegriffen werden darf, kann von der Exekutive festgelegt werden, ein weiteres Gesetz wäre nicht notwendig. Was das mit dem Schutz von Kindern vor sexuellem Mißbrauch zu tun hat, bleibt allerdings offen.

[1] *Richtlinie Des Europäischen Parlaments Und Des Rates* über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation

inoffizielle Version (englisch):

http://www.gilc.org/as_voted_2nd_read.html

offizielle Version in: „Angenommene Texte, Sitzung vom 30.05.2002“, Seiten 12ff.

http://www3.europarl.eu.int/omk/omnsapir.so/calendar?APP=PDF&TYPE=PV2&FILE=p0020530DE.pdf&LANGUE=DE

[2] Gesetz zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen (zur Zeit nicht verfügbar)

http://www.parlamentsspiegel.de/cgi-bin/hyperdoc/show_dok.pl?k=BBD275/02

[3] so z.B. Michael Holstein, Interpol, in einem Interview mit der c't, Ausgabe 12/2002

[4] Presseerklärung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zur Bundesratsinitiative

http://www.datenschutzzentrum.de/material/themen/presse/kommunik.htm

[5] Interview mit Telepolis, Magazin der Netzkultur

http://www.heise.de/tp/deutsch/inhalt/te/12661/1.html

[6] Agenda des Europol-Expertentreffens vom 11.04.2002

http://www.radicalparty.org/europol/europol.pdf

SNoRT – the Open Source Intrusion Detection System

von Bastian Ballmann *<bytebeater@crazydj.de>*

Snort ist ein Network Intrusion Detection System und wurde ursprünglich von Marty Roesch entwickelt. Wie das aber bei größeren Open Source Projekten so üblich ist, wird Snort mittlerweile von einer größeren Entwicklergemeinde gepflegt und weiter entwickelt. Firmen wie Silicon Defense (SnortSnarf) oder das CERT Institut (ACID) sind wohl die besten Beispiele. Die aktuellen Sourcen gibt es unter [1].

Dieser Artikel über Snort soll nicht erklären wie man Snort an sich konfiguriert. Die Configdatei selbst gibt einem schon viele Information und zu diesem Thema findet man auch genügend gute Resourcen im Netz, ein paar davon findet man in den Referenzen am Ende dieses Artikels. Der Artikel soll einem viel mehr die Tools um Snort herum näher bringen (z.B. wie man Attacken, die Snort entdeckt hat automatisch abwehren kann), was Snort kann und was nicht, einen groben Überblick über den Aufbau von Snort bieten und erklären wie man Snort durch eigene Regelwerke erweitern kann und wo man das IDS plazieren sollte oder wie man Statistiken über die Angriffe erstellen kann.

Wie arbeitet Snort?

Snort schaltet das Netzwerk Interface in den Promisc Modus und bedient sich der berühmten libpcap Bibliothek, um die vorbei fliegenden Packete zu sniffen. Die abgefangenen Packete werden dann einmal über Plugins disassembled (Einstellungssache) und der Payload mit einer Vielzahl von verschiedensten Rulesets verglichen. Die Rulesets bestehen aus Packetbeschreibung, wie sie bei bestimmten Angriffen auftreten. Das heisst aber nicht, daß Snort nur bekannte Angriffe auf Protokolle und Exploits erkennen kann. Snort spürt genauso "illegale" Packete auf wie z.B. ein TCP Packet mit einer TTL von 0 oder Port 0, bemerkt DOS / DDOS Attacken oder unnormalen Netzwerkverkehr (Plugin Spade). Desweiteren kann Snort über viele Plugins erweitert werden. Diese Plugins können z.B. Portscans entdecken, den Code einer Telnet Session analysieren, Unicode codierten Payload decodieren oder CGI NULL Byte Attacken aufspüren. Die Möglichkeiten sind vielfältig! Diese Plugins sorgen auch dafür, daß der Payload für Packete von und / oder zu bestimmten Ports auf einem bestimmten Layer disassembled und analysiert werden können. Diese gefundenen bösen Packete kann Snort auf die unterschiedlichsten Wege loggen und an den Mann / Admin bringen: XML, Datenbank, tcpdump Format, Snort Binary Format oder traditionell über Syslog. Das sollten erstmal genug Informationen über die Arbeitsweise von Snort sein. Wie gesagt ich werde hier nicht auf die Configuration von Snort eingehen und setze ab diesem Zeitpunkt voraus, daß Du ein mehr oder weniger gut configuriertes Snort IDS vor der Nase hast! Und als letzte Anmerkung: Der Artikel beschäftigt sich mit Snort unter Linux. Ich weiß, daß es Snort auch für Win32 Systeme gibt, aber ich habe bisher keinen besonderen Sinn darin gesehen mich damit zu beschäftigen und kann deswegen auch nicht dafür garantieren, dass die behandelten Zusatztools alle unter Windows laufen! Für Windows Benutzer gibt es aber ein schönes GUI (ids_center) für die Configuration von Snort.

Snort Placement

Wo darf ich das Schwein denn parken? =) Natürlich ist es auch entscheident in welcher Stelle des Netzwerks Snort eingebunden wird, denn es versteht sich glaube ich von selbst, dass das beste NIDS nichts bringt, wenn man sich an ihm vorbei mogeln kann. Deshalb ist es eine gute Idee das NIDS System direkt auf dem Gateway laufen zu lassen, voraus gesetzt es gibt keine weitere Verbindung zum Internet bzw. zu einem anderen unsicheren Netz. Dadurch kann man auch einige Angriffe von intern erkennen, wenn z.B. der firmeneigene Mailserver gehackt wird, um die Mails von anderen Mitarbeiter zu lesen.

Internes Netz -->-- Gateway + Snort -->-- DMZ --<-- Firewall --<-- Internet

Nehmen wir mal an das Netzwerk sieht folgendermaßen aus und in der DMZ stehen Webserver, die vom Internet aus durch eine weitere Firewall geschützt werden. Dann sollte die Firewall natürlich auch ein Intrusion Detection System enthalten, weil sie ja der

einzige Weg in die DMZ und das dahinter liegende interne Netz ist. Die meisten kommerziellen Firewall Systeme bieten das mittlerweile auch an. Es ist auch nicht verkehrt in der DMZ selber ein weiteres NIDS zu installieren, um Angriffe und Anormalitäten zwischen den Webservern zu erkennen oder aber IIS und Apache Webserver getrennt zu überwachen. Man kann das IDS der Firewall auch so einstellen, daß es nicht die Ports 80 und 443 überwacht und diese Arbeit dem NIDS in der DMZ überläßt, weil vom Internet zu viel Traffic kommt. Genauso kann man Snort zwischen zwei Abteilungen im internen Netz schalten, um z.B. einen Angriff eines Programmierers auf die Datenbank der Personalabteilung zu erkennen und ab zu wehren, damit der nicht seinen Gehaltseintrag verbessert oder so... =) Je nachdem wo Snort so rum steht, scannt man natürlich auch andere Packete und läßt andere Sachen unkontrolliert passieren, was sich sehr positiv auf die Performance auswirken kann. Obwohl Snort ist so oder so verdammt schnell unterwegs, man bemerkt es eigentlich gar nicht, nur wenn der Traffic massiv hoch ist, kann es sich eventuell störend auswirken. Weiterführende Literatur gibt es unter [2].

Intrusion Detection != Intrusion Prevention?

Es ist ja schön und gut, daß Snort mir sagen kann wie und wann ein Angriff auf mein Netzwerk stattgefunden hat, es kann mir allerdings nicht sagen, ob der Angriff erfolgreich war oder nicht und wäre es nicht auch viel schöner wenn man den erkannten Angriff gleich verhindern könnte?? Man kann, also sollte man es auch tun! Dazu bedienen wir uns des Perl Scripts Guardian (liegt dem Snort Packet bei, ansonsten gibt es eine aktuellere Version auf [1]). Guardian macht nichts anderes als die Logdatei von Snort nach Attacken zu durchsuchen und die IP des Angreifers über ipchains oder IPtables zu sperren. Dabei kann man Guardian auch ein Timeout für die Sperre mitteilen und eine Ignore Liste anlegen, damit nicht die eigenen Rechner gesperrt werden oder der Nameserver, der gerne für False Alarms sorgen soll (laut Guardian Dokumentation, stimmt nicht unbedingt mit meinen Erfahrungen überein). Die Configuration von Guardian ist total simpel und wird auch in der Dokumentation sehr gut beschrieben, deswegen werde ich hier auch darauf nicht weiter eingehen. Zu erwähnen ist allerdings noch, daß man sein IDS schon gut configuriert haben sollte, also mit so wenig false alarms wie nur irgend möglich, weil man ansosnten ungewollt auch unschuldige Maschinen blockt. Guardian loggt natürlich auch wann er wen und warum gesperrt hat.

Snort Logging

Snort loggt unter Umständen viele Attacken auf dem Rechner. Diese Flut an Informationen will man natürlich auch so gut wie möglich verarbeiten. Dazu gibt es die unterschiedlichsten Programme. SnortSnarf kann über ein CGI Programm die Logdaten in HTML präsentieren und auch schon ein paar statistische Daten liefern wie z.B. eine Top 20 der Source bzw. Destination IPs mit den meisten Angriffen. Man bekommt eine Zusammenfassung aller Angriffsarten und kann sich die betroffenen IPs und sonstigen Daten schön aufbereitet anschauen. Ich habe auch selbst mal ein kleines Perl Script geschrieben, daß einfach nur hin geht und die Snort Logdatei nach neuen interessanten Einträgen durchforstet und sie an einen oder mehrere Admins per Mail schickt. Interessant heisst in diesem Zusammenhang man bekommt alle Logdaten zu geschickt, von denen das Tool icht weiß, dass sie einen _nicht_ interessieren. Das Script findet man unter http://members.tripod.de/bytebeater/snortmailer.zip Man kann allerdings auch die Logdaten in eine Datenbank wie z.B. MySQL oder Postgesql schreiben lassen, um sie nachher für Statistiken zu gebrauchen... Dazu muss man in der snort.conf nur das Datenbank Plugin einschalten und mit Parametern versorgen: output database: log, mysql, user=snort password=snort dbname=snort host=localhost detail=full encoding= ascii Dieser Eintrag würde die Logs in eine MySQL schreiben. Die Packetinformationen sollen detailliert also auch mit dem enthaltenen Payload in ASCII geloggt werden. Dadurch kann man vielleicht selbst noch ein paar neue Angriffstechnicken erlernen, während man im Hintergrund die Packete droppt... =) Die Beschreibung zu dem Datenbankschema gibt es unter [3].

Snort Statistik

Wenn man seine Logdaten nicht in eine Datenbank schreibt, kann man das Perl Script snort_stat.pl verwenden, um Statistiken von seinen Logs zu erstellen. Das Programm zeigt einem an welche Attacken am meisten auf den Rechner / das Netzwerk niederprasseln oder von welchem Adressraum die meisten Attacken gestartet werden. Desweiteren kann man fest stellen wie viele Attacken insgesamt auf das Netzwerk gefahren wurden und welcher der Rechner am meisten angegriffen wurde. Wenn man über logrotate seine Logfiles täglich rotiert, dann kann man auch ganz leicht heraus finden an welchen Wochentagen man am meisten angegriffen wird. Wenn man das Spade Plugin verwendet, dann kann man auch sehen zwischen welchen Rechnern die meisten merkwürdigen (unnormalen) Pakete hin und her geschickt wurden. Schreibt man seine Logdaten dagegen in eine Datenbank und hat einen Apache mit PHP Unterstützung zur Verfügung, dann kann man auch das excellente Programm ACID (Analysis Console for Incident Databases) vom CERT Institut verwenden. Mit ACID kann man sich Statistiken darüber erstellen, in welchen Stunden, an welchen Tagen bzw. Monaten / Jahren die meisten Angriffe statt gefunden haben. Natürlich auch welches die meisten Angriffe waren und von welchen Adressbereichen. Das Ergebnis kann grafisch aufbereitet werden. Man kann sich auch

anzeigen lassen über welche Protokolle die meisten Attacken gefahren wurden oder was die letzten 5 Angriffe oder die Angriffe in den letzen 24 Stunden waren. Fast schon selbst verständlich kann man sich auch Select Statements zusammen klicken, um Angriffe mit bestimmten Kriterien zu suchen. Die Ergebnisse kann man sich auch per Mail zu schicken und es gibt die Möglichkeit Angriffe zu Alert Groups zusammen zu fassen. Mit letzerem hab ich allerdings noch nicht gespielt... Auf der Homepage von ACID [4] wird auch auf ein weiteres Tool hingewiesen: logsnorter. Dieses Perl Script läuft im Hintergrund und schreibt alle über die Firewall (IPtables, ipchains, ipfwadm...) gedroppten Packete in die Snort Datenbank, damit man sich mit ACID ein noch besseres Bild über die wirklich auf den Rechner / das Netzwerk niederprasselnden Angriffe machen kann. Zum Schluss noch schnell ne kleine Warnung: Wenn Du auf Snort 1.8.6 updatest, dann musst Du unbedingt auch ACID updaten, weil sich das Datenbankschema anscheinend leicht geändert hat. Um genau zu sein "nur" die Tabelle iphdr, die alle IP Header Informationen beinhaltet. Zumindest will meine ACID Version 0.9.6b11 immer auf Spalten wie ip_src0 zu greifen und die gibt es nicht... Fazit: ACID ist genial!!! Du solltest es auf jeden Fall ausprobieren, weil wenn Du es einmal gesehen hast, dann kommst Du schon von alleine drauf, dass Du es nicht mehr missen möchtest... ;)

Hacking Snort

Vor und während des CCC Easterhegg Congresses hab ich mal Snort einfach so laufen lassen, während ich meine TCP Hijacking Angriffe ausprobiert habe und ich musste zu meinem Entsetzen fest stellen, dass Snort nichts mit bekommt, wenn man sich nicht völlig blöd anstellt. Voll blöd wäre in diesem Fall ein generiertes TCP Packet mit TTL 0 oder einem bestimmten Windowsize Wert, den Snort dann als einen bestimmten Angriff eines Tools erkennt, weil dieses Tools halt die Eigenschaft hat, Packete mit genau dieser Windowsize zu generieren. Ein RST Daemon bleibt allerdings völlig unentdeckt. Ich habe auch ein wenig mit dem SPADE Plugin rum gespielt und das konnte diese Situation leider nicht verbessern, obwohl es garantiert unnormal ist, wenn man von einem Server zuerst ein (gespooftes) RST Packet zurück bekommt und danach ein ACK oder SYN/ACK Paket. Last but not least ist der ARP Spoof Preprocessor (von Snort 1.8.3) völliger Schrott, weil er hat noch nicht einmal gepeilt, dass ich mit hunt jede Sekunde einen ARP Poisoning Attack abfeuer! Geschweige denn etwas von weniger auffallenderen Attacken mitbekommen. Sollte ich mit dieser Behauptung falsch liegen, korrigier mich bitte und sag mir wie Du den ARP Preprocessor configuriert hast! Außerdem müssen die gesammelten Log Daten immernoch von einem Admin ausgewertet werden und auf dem Easterhegg Congress hat auch jemand ein Tool vorgestellt, das aus den Paketbeschreibungen der Rulesets Pakete erstellt und diese dann Snort vor die Schnauze wirft. Die enstehenden Logs kann man nicht mehr besonders sinnvoll auswerten und somit kann ein Angreifer in dieser Datenflut untergehen. Vorausgesetzt seine Pakete kommen an und werden nicht über Guardian entsorgt. Als letzes möchte ich hier noch kurz auf den CGI Scanner Whisker von RFP eingehen. Abgesehen davon, dass ich Whisker für den besten CGI Scanner halte, versucht das Tool durch verschiedene Technicken IDS System zu umgehen. Die Ideen wie Hex codierte URLs oder Double-Shlashes in der URL sollten die Regelwerke eines IDS aus tricksen. Die Ideen fand ich recht interessant und somit hab ich Whisker mal auf Snort los gelassen. Das Ergebnis kann sich sehen lassen: Snort kann man dadurch nicht verarschen! =)

Snort erweitern

Wenn man auf einen neuen Exploit gestossen ist und möchte, dass Snort diesen auch erkennen kann, dann sollte man sich ein eigenes Ruleset schreiben bzw. ein bestehendes erweitern. Es versteht sich hoffentlich von selbst, dass die neuen Rules der Snort Gemeinde zur Verfügung gestellt werden... Um ein einfaches Beispiel zu nehmen, schreiben wir uns jetzt mal eine Paketbeschreibung, die alle RST Packete mit Window size 1024 als gefährlich einstuft.

```
Tcpdump 16:06:03.326371 syntaxerror.crazydj.d
e.6666 > gateway.crazydj.de.http: R 0:2(2) win
1024 [tos 0x10]
```

```
Snort Rule alert tcp $EXTERNAL_NET any <>
$HOME_NET any (msg:"Detected packet with
window-size 1024; flags:R; classtype:misc-
activity; rev:5;)
```

Unter diese Regel fällt ein TCP Packet, dass entweder vom externen Netz ins interne Netz oder umgekehrt geschickt wird (Port any), das RST Flag (und nur das RST Flag) gesetzt hat und eine Windowsize von 1024 aufweist. Als Logmeldung wird daraufhin der msg String in die Logdatei geschrieben. Als nächstes soll das Paket nur geloggt werden, wenn es von dem Rechner syntaxerror and gateway geschickt wird, anders herum interessiert uns nicht und um die Sache noch etwas spannender zu gestalten, muss das Paket noch den Payload "CCC TCP Hijacking is not a crime" enthalten. Der Rechner Syntaxerror hat die IP 192.168.0.1 und Gateway die 192.168.0.2.

```
Tcpdump 16:09:26.017503 syntaxerror.crazydj.
de.6666 > gateway.crazydj.de.http: R 0:30(30)
win 1024 [tos 0x10] 0x0000     4510 0046 419a
0000 1906 d876 c0a8 0321      E..FA.....v...!
0x0010  c0a8 0320 1a0a 0050 0000 0000 0000
0000   .......P........ 0x0020
 5004 0400 75bb 0000 4343 4320 4869 6a61
P...u...CCC.Hija 0x0030        636b 696e 6720
6973 206e 6f74 2061 2063      cking.is.not.a.c
0x0040 7269 6d65 0d0a
rime..
```

```
Snort Rule alert tcp 192.168.0.1 any ->
192.168.0.2 any (msg:"Detected packet with
window-size 1024; flags:R; content:"CCC
Hijacking is not a crime"; classtype:misc-
activity; rev:5;)
```

Um die Packetbeschreibung so genau wie möglich zu gestalten und false alarms zu vermeiden, wollen wir das Packet jetzt nur loggen, wenn es als Destination Port 80 eingetragen hat

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 80
(msg:"Detected packet with window-size 1024;
flags:R; content:"CCC Hijacking is not a
crime"; classtype:misc-activity; rev:5;)
```

Die Ausdrücke können natürlich auch über den ! Operator netgativ formuliert werden, also wenn das Paket nicht nach Port 80 geschickt wird. Oder aber wenn das Packet an einen Port kleiner als 1024 geschickt wird, dann sähe die Regel so aus:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET:
1024 (msg:"Detected packet with window-size
1024; flags:R; content:"CCC Hijacking is not a
crime"; classtype:misc-activity; rev:5;)
```

Es gibt noch eine ganze Reihe weitere interessante Befehle wie z.B. ttl, nocase, seq, ack, dsize usw... Die offizielle Snort Dokumentation enthält eine gute Referenz dazu [5]. Ob die Regeln auch wirklich funktionieren kann man sehr gut mit meinem Packetgenerator kontrollieren [6]. Ansonsten hält man seine Snort Rules am besten mit dem Programm oinkmaster auf dem neuesten Stand. Das Perl Script gibt es unter [7] Allerdings ist oinkmaster noch auf die alte Homepage Struktur von snort.org eingeschossen, deswegen muss man ihm immer mit dem Parameter -u die neue URL [8] unterschieben.

Referenzen

Offizielle Snort Homepage *http://www.snort.org*

Snort Mailing Listen *http://www.snort.org/lists.html*

Snort im Usenet *mailing.unix.snort*

The Lisa Paper *http://www.snort.org/docs/lisapaper.txt*

Beschreibung nützlicher Snort Tools und Addons *http://members.tripod.de/bytebeater/snort-toolz.html*

Where to place a Snort IDS *http://www.snort.org/docs/scott_c_sanchez_cissp-ids-zone-theory-diagram.pdf*

Snort VS Whisker CGI Scanner *http://online.securityfocus.com/infocus/1577*

Virtual Honeynets *http://online.securityfocus.com/infocus/1506*

Snort Installation and Basic Usage *http://online.securityfocus.com/infocus/1421*

Identifying ICMP Hackery Tools Used In The Wild Today *http://online.securityfocus.com/infocus/1183*

Links

[1] *http://www.snort.org*

[2] *http://www.snort.org/docs/scott_c_sanchez_cissp-ids-zone-theory-diagram.pdf*

[3] *http://www.snort.org/docs/snortdb.png*

[4] *http://acidlab.sourceforge.net*

[5] *http://www.snort.org/docs/writing_rules/*

[6] *http://ip-packet.sourceforge.net*

[7] *http://www.algonet.se/~nitzer/oinkmaster/*

[8] *http://www.snort.org/dl/signatures/snortrules.tar.gz*

Greets

Stefan Krecher DocX Pylon Harald Land Uli Klenk Stefan Mähler Maik Schröder Roland Schuppin Saluto Dj Ecki

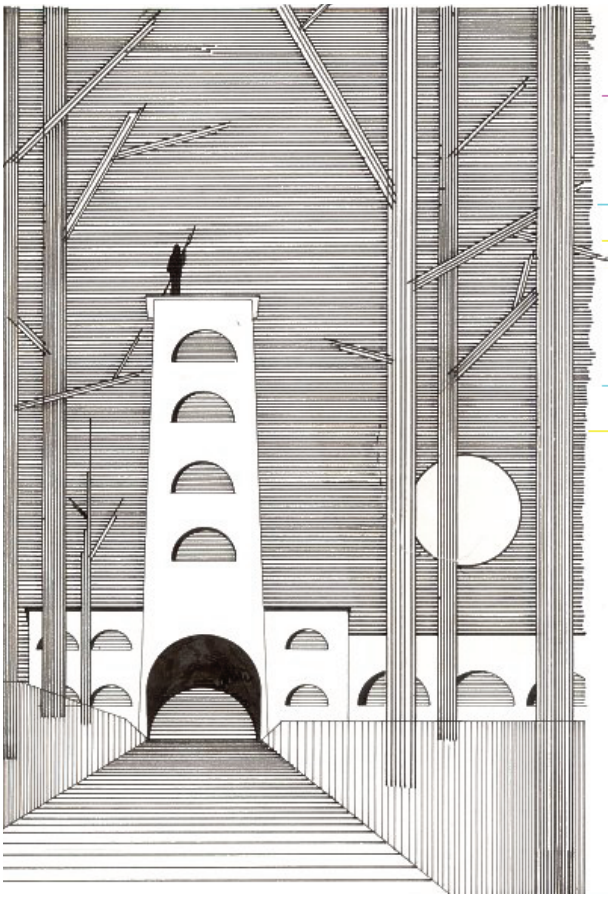

```
/* Happy Snorting out there! =) */ // [EOF]
```

Plakatmotiv auf der NRW-Demo, photographiert von Horst Walter Schwager

Hackerethik 2002

Autor: R.Schrutzki

Seit meinem letzten Beitrag zu diesem Thema sind vierzehn Jahre ins Land gegangen und die Szene hat sich gründlich gewandelt, so scheint es jedenfalls auf den ersten Blick. Da gibt es auf einmal Hacker, Neohacker, Dark Side Hacker, Script Kiddies, Crackers, Lamers, Phreakers, warez doodz und so weiter. Die ganze Palette des alternativen Computereinsatzes wird von der öffentlichen und der veröffentlichten Meinung in einen Topf geworfen, während die Gruppen selber nichts besseres zu tun haben, als sich voneinander abzugrenzen.



Unterdessen ist das Raubkopieren von Programmen, Musik und Video zum Volkssport Nummer Eins geworden, bei dem sich niemand mehr etwas Böses denkt und die Rechte der Dateninhaber aufs Gröbste missachtet werden. Chaos überall :-)

Nun sind Strukturen etwas, das sich nur aus dem Chaos entwickeln kann und es stellt sich die Frage, was für Strukturen das sein können, die zumindest für so etwas wie Überschaubarkeit sorgen können und das Selbstverständnis begreifbar machen. Dabei sind sicher flexible Strukturen angesichts der rasanten Veränderung geeigneter, als starre, und diese flexiblen Strukturen gilt es zu stützen.

Wenn wir uns die ursprünglich von Stephen Levy dokumentierte Hackerethik ansehen, finden wir so eine flexible Struktur, die mit nur sechs Statements eher eine Weltanschauung propagiert, als Regeln vorzugeben. In dieser Struktur könnten sich mühelos alle oben genannten Gruppen wiederfinden, wenn sie denn wollten und die jeweils anderen es zuliessen. Alleine der Grundsatz, dass alle Information frei und unbeschränkt sein soll, öffnet jeder Art von Bitschieberei Tür und Tor, der nur die Selbstorganisation Einhalt gebietet. Was ja auch gut zur informationellen Selbstbestimmung passt, in der jedem freisteht, zu

entscheiden, welche Informationen er weitergibt, welche er benötigt und für welche er gegebenenfalls eine angemessene Belohnung spendiert. Interessant in diesem Zusammenhang auch die Tatsache, dass das ursprüngliche weiche "soll" des Statements inzwischen einem harten "muss" gewichen ist. Ist hier die Evolution am Werk gewesen, oder hat da jemand Orwells "Farm der Tiere" zu gut verinnerlicht?

Ende der achtziger Jahre war der Druck auf die damalige Hackerszene recht stark, was zu einem Teil von ihr selber verschuldet war. Es gab zwei Strömungen, die sich beide auf ihre Art und Weise mit den verschiedensten Geheimdiensten einliessen. Während die einen zwecks Schadensbegrenzung mit dem BND kooperierten, liessen sich die anderen aus noch fragwürdigeren Motiven auf den KGB ein, mit den bekannten Ergebnissen. Die Frage, warum man sich denn überhaupt mit diesen fragwürdigen Organen staatlicher Macht einlassen solle, wurde nie hinterfragt. Im Ergebnis jedoch wurde das öffentliche Bild vom Hacker als Schadensstifter verstärkt und eine Abgrenzung für erforderlich gehalten. Dieses erste Schisma der deutschen Szene findet sich symbolhaft im derzeitigen siebten Statement der Hackerethik wieder und ist nicht nur ein radikaler Wandel der Hackerethik, weg vom Weltanschaulichen und hin zu klaren Verhaltensvorschriften, sondern auch typisch Deutsch. "Mülle nicht in den Daten anderer Leute" lautet der Befehl und man hat sich daran zu halten. Die galaktische Vereinigung ohne feste Strukturen hatte eine feste Struktur geschaffen, die seinerzeit von mir auch mitverantwortet wurde.

Dieses siebte Statement ist auch inhaltlich nicht unproblematisch, da es das "Müllen" gar nicht definiert. Ist nicht strenggenommen schon der Login-Versuch danach verboten, da er ja Datenspuren im Logfile hinterlässt (und das Aufräumen des Logfiles hinterher ist auch ein Eingriff in fremde Daten :-) oder müsste man das Statement nicht besser, wiederum in bester Orwellscher Manier, ein wenig ergänzen und klarmachen, dass es sich nur auf persönliche Daten beziehen kann? Aber man wollte damals um jeden Preis das Bild des lieben Hackers propagieren und schuf so praktisch erst den Begriff des Dark Side Hackers, zu denen ich ich dann wohl im Nachhinein nach dieser Definition auch gehöre, obwohl ich mich nie so gesehen habe und mich immer nach der bis dahin geltenden Ethik verhalten habe. Auch dass schon die ersten Hacker vom TMRC <http://tmrc.mit.edu/hackers-ref.html> es bei der Verfolgung ihrer Interessen mit der herrschenden Ethik nicht so genaunahmen, und die Dioden für ihre Schaltungen einfach klauten, lässt man heute gerne unter den Tisch fallen, um jeden Grauzonenverdacht auszuschalten.

Auch das achte Statement, wieder mehr Verhaltensmassregel als ethische Grundlage, ist nicht unproblematisch und operiert meines Erachtens mit den falschen Begriffen. "Öffentliche Daten nützen, private Daten schützen" soll dem Schutz der Privatsphäre

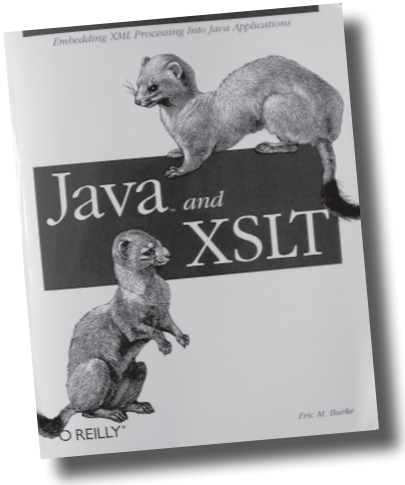
dienen, übersieht aber völlig, dass private Daten sehr wohl auch öffentlich sein können, zum Beispiel wenn es sich bei diesen Daten um ein Musikstück oder Ähnliches handelt. Der Begriff privat wäre sicher auch besser durch das Wort persönlich zu ersetzen, dann das ist es, was ich als Dateninhaber auch dann geschützt wissen möchte, wenn ich nicht die Verfügungsgewalt habe. Hier wird deutlich, dass der Konflikt zwischen freier Information und Urheberrecht noch immer nicht befriedigend abgedeckt werden kann und man hätte es besser bei dem Grundsatz der Informationsfreiheit belassen, der mit seinem ursprünglichen "soll" ja durchaus auch die Ausnahme der persönlichen Daten zulässt.

Insgesamt finde ich den Versuch, eine Hackerethik durch zusätzliche starre Regeln ihrer Flexibilität zu berauben, eher ungeschickt. Vielleicht ist das eine Deutsche Eigenart, dass man immer Vorschriften macht oder haben will. Ich für mein Teil habe mich wieder auf die ursprüngliche Hackerethik besonnen, ich habe schliesslich auch schon ganz gut nach ihr gelebt, als ich sie noch gar nicht kannte. Bestimmte Werte sind eben nicht durch starre Regeln anzuerziehen, sondern nur durch Begreifen erfahrbar.

Hinweis: Dieser Text ist dynamisch, das heisst in Arbeit. Version 23.00 vom 10.4.2002; die Illustrationen stammen vom Autor http://www.schrutzki.net/bilder/grafik/schwarzweiss.html

Java und XSLT

von Eric M. Burke



Ein unter Hackern weit verbreitetes Phänomen ist ja bekanntermaßen die sog. "Buzzword-Allergie" – je mehr Buzzwords ein Produkt enthält, umso mißtrauischer wird ihm begegnet.

Da ist die Besprechung eines Buches mit dem Titel "Java and XSLT" in der Datenschleuder ja geradezu provokant, geniessen doch gleiche beide Technologien den zweifelhaften Ruf langsam, ressourcenfressend, unnötig komplex und realitätsfern zu sein.

Zumindest mit den letzten beiden Vorurteilen möchte Eric M. Burke mit seinem Buch aufräumen. Das tut er auch -- und zwar gründlich... Das Buch ist in erster Linie für Java-Programmierer gedacht, die schnell zu "Hands-On-Experience" mit XSLT und XML kommen möchten. Der Schwerpunkt liegt bei zielplattformunabhängigen Publishing Anwendungen, viele der Beispiele sind als Servlets realisiert und benutzen Tomcat als Referenzumgebung, aber auch ein XSLT Transformer GUI, das mit Swing arbeitet, ist zu finden.

Obwohl in den Kapiteln eins, vier und sechs mit genügend theoretischen Hintergrundinformationen zu den Themen Java Web Technologies, XML und XSLT aufgewartet wird, um auch einem Anfänger einen Einstieg in die Materie zu ermöglichen, stehen in den restlichen (sieben) Kapiteln vor allem praktische Beispiele und Tips aus der Praxis im Vordergrund.

Damit hebt sich das Buch wohltuend von vielen Veröffentlichungen ab, die hauptsächlich auf die konzeptionellen Vorteile von Java und XML abzielen und ansonsten gerne in Allgemeinplätzen verweilen ("Java ist klasse, weil es plattformunabhängig ist. XML auch. Alle großen Firmen benutzen es. Die müssen es ja wissen. Details siehe java.sun.com und www.w3c.org. Vielen Dank, dass Sie für dieses Buch $79.90 gezahlt haben. Gehen Sie nicht über Los, ziehen Sie nicht 400 Mark ein.")

Das bedeutet unter anderem auch, dass auch auf Probleme bei der Installation der benötigten Java-Packages eingegangen wird (Stichwort "CLASSPATH-Hölle") und ein eigenes Kapitel (das neunte) den Aspekten Deployment, Debugging und Performance gewidmet ist. Die Codebeispiele sind einerseits klein genug gehalten, um eine detaillierte Besprechung zu erlauben, andererseits aber funktional und praktisch genug, um als Ausgangsbasis für eigene Projekte herzuhalten.

Insbesondere das siebte Kapitel, welches Design, Implementierung und Deployment eines (rudimentären) Diskussionsforums von Anfang bis Ende beschreibt, zeigt, dass ein Java- und XSLT-basierter Ansatz nicht zwangsläufig zu "Bloat-Code" führen muss.

Das Buch hat zwar insgesamt eher den Charakter eines Tutorials, als den eines Nachschlagewerkes (der Referenzteil zur Java XML API JAXP und zur XSLT-Syntax nimmt schmale fünf Prozent des Seitenumfanges ein), kann aber trotzdem auch nach dem Durchlesen durchaus Verwendung im Alltag finden. Immer dann nämlich, wenn man wieder mal eine Standardfunktionalität implementieren muss ("Wie komme ich nochmal von einer URI zum geparseden Stylesheet?", "Wo definiere ich Laufzeitparameter, die ich dann wie nachher vom Servlet an mein Stylesheet weiterreiche?" usw.), dann ist es durchaus schneller, das fertige Beispiel im Buch nachzuschlagen, anstatt sich durch fünf, sechs JavaDoc Einträge – auf zwei bis drei Packages verteilt – durchzuklicken.

Wer also seine Buzzword-Phobie überwunden hat und mit Java XML verarbeiten möchte (mittels XSLT, natürlich), dem sei dieses Buch hiermit ans Herz gelegt.
<Tom Lazar>

Eric M. Burke: Java und XSLT, O'Reilly, 2001, ISBN 0-596-00143-6

Bestellungen, Mitgliedsanträge und Adressänderungen bitte senden an:

CCC e.V., Lokstedter Weg 72, D-20251 Hamburg, Fax +49.40.401.801.41

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

- Chaos CD Blue, alles zwischen 1982 und 1999 EUR 23 + EUR 3 Porto
- Alte Ausgaben der Datenschleuder auf Anfrage
- Datenschleuder-Abonnement, 8 Ausgaben
  Normalpreis EUR 32
  Ermäßigter Preis EUR 16
  Gewerblicher Preis EUR 50 (wir schicken eine Rechnung)
- Satzung und Mitgliedsantrag
  EUR 2,50 oder zum Selberausdrucken unter *http://www.ccc.de/club/membership*

Die Kohle

- liegt als Verrechnungsscheck bei
- wurde überwiesen am _____._____._____ an

  Chaos Computer Club e.V., Konto 59 90 90-201
  Postbank Hamburg, BLZ 200 100 20

Name: _____

Straße / Postfach: _____

PLZ, Ort _____

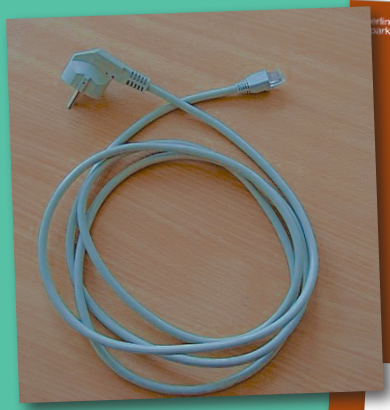
Tel.* / Fax* _____

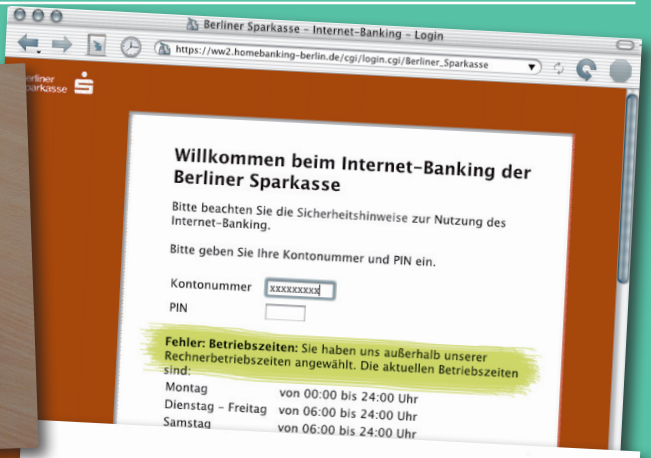
E-Mail: _____

Ort, Datum: _____

Unterschrift _____

*freiwillig




Berliner Sparkasse - Internet-Banking - Login
https://ww2.homebanking-berlin.de/cgi/login.cgi/Berliner_Sparkasse
Willkommen beim Internet-Banking der Berliner Sparkasse
Bitte beachten Sie die Sicherheitshinweise zur Nutzung des Internet-Banking.
Bitte geben Sie Ihre Kontonummer und PIN ein.
Kontonummer
PIN
Fehler: Betriebszeiten: Sie haben uns außerhalb unserer Rechnerbetriebszeiten angewählt. Die aktuellen Betriebszeiten sind:
Montag von 00:00 bis 24:00 Uhr
Dienstag - Freitag von 06:00 bis 24:00 Uhr
Samstag von 06:00 bis 24:00 Uhr


Internet-Wortschatz
I apologize for this latest entry. I can't find a chimp making a face as dumb as this one.
-Rich
Chaos Computer Club
[kehoss kəmpjuhtə klab]
Ein in Deutschland eingetragener Verein, der aus einer Gruppe von Hackern (>hacker) besteht, welche durch das Eindringen in fremde Computernetze auf die Sicherheitsrisiken und Gefahren der vernetzten Gesellschaft hinweisen wollen.
character
[kärrəktə]
Schriftzeichen
Binäre (>binary) Darstellung eines Buchstabens,