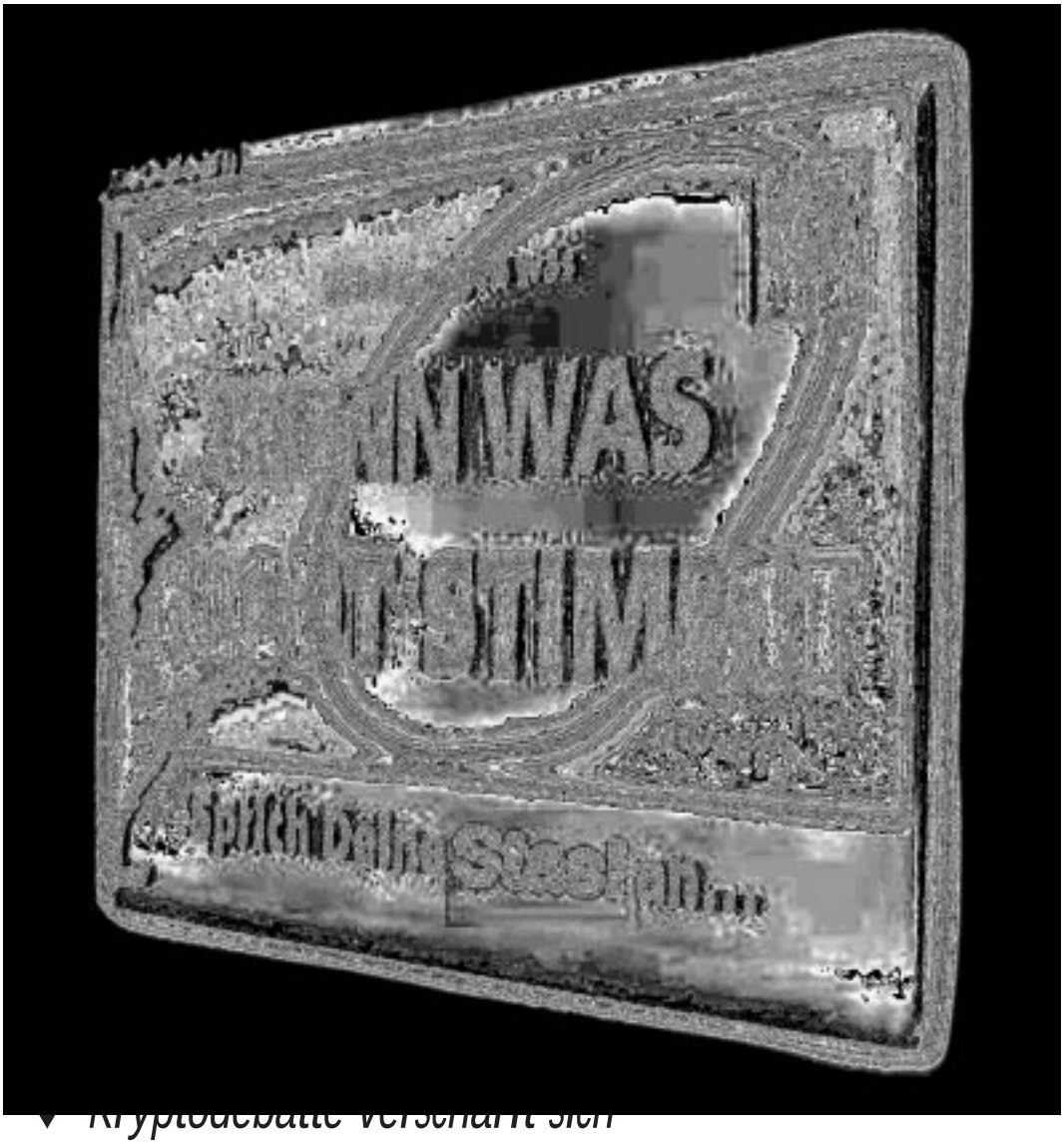
Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club



- *Kryptodebatte verschärft sich*
- *Im Fadenkreuz: SAP R/3*
- *Dokumentation Congress '97*

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

#62

Impressum

Die Datenschleuder Nr. 62
I. Quartal, März 1998

Herausgeber:
(Abos, Adressen etc.)
Chaos Computer Club e.V.,
Schwenckestr. 85, D-20255 Hamburg,
Tel. +49 (40) 401801-0,
Fax +49 (40) 4917689,
EMail: office@ccc.de

Redaktion:
(Artikel, Leserbriefe etc.)
Redaktion Datenschleuder,
Postfach 642 860, D-10048 Berlin,
Tel +49 (30) 285 986 00
Fax +49 (30) 285 986 56
EMail: ds@ccc.de

Druck: St. Pauli Druckerei Hamburg
ViSdP: Andy Müller-Maguhn

Mitarbeiter dieser Ausgabe:
Andreas Bogk (andreas@ccc.de), Andy Müller-Maguhn (andy@ccc.de), Frank Rieger (frank@ccc.de), Tim Pritlove (tim@ccc.de), Tobias (tobias@ccc.de), Wau Holland (wau@ccc.de)

Adressen

Info: http://www.ccc.de
Diskussion: de.org.ccc
Anfragen: ccc@ccc.de

Erfa-Kreise des CCC

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

Berlin: Club Discordia Donnerstags alle zwei Wochen 17-23 Uhr in den Clubräumen, Marienstraße 11, Hinterhof, Berlin-Mitte, Nähe Bahnhof Friedrichstraße, Tel. (030) 28598600, Fax (030) 28598656, EMail: ccc@berlin.ccc.de. Briefpost: CCC Berlin, Postfach 642 860, D-10048 Berlin.

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

Sachsen/Leipzig: Treffen jeden Dienstag ab 19 Uhr im Café Ambiente, Petersteinweg, Nähe Neues Rathaus/Hauptpolizeiwache. Veranstaltungen werden p. Mail über den Sachsen-Verteiler (Uni-Leipzig) angekündigt. Infos für Neueinsteiger gibt´s von bubble@sachsen.ccc.de. Briefpost: Virtueller CCC-Sachsen, c/o Frohburger Medienhaus, Leipziger Str. 3, 04654 Frohburg, Tel: (034348) 51153, Fax (034348) 51024, EMail: sachsen@ccc.de, http://www.sachsen.ccc.de

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

Köln: Treff jeden Dienstag um 19:30 im ChaosLabor, Bobstraße 28 (Ecke Clemensstraße), 50676 Köln.
http://koeln.ccc.de, EMail: info@koeln.ccc.de.

Mönchengladbach: Treff: Surfer's Paradise, Bahner 19 in Mönchengladbach vorerst einmal im Monat jeden letzten Freitag, Ab 1. August dann immer Dienstags um 20 Uhr. EMail: gregor@enconet.de

Ulm: Treff jeden Montag um 19 Uhr im Cafe Einstein an der Uni Ulm. Kontakt: frank.kargl@rz.uni-ulm.de.

Frankfurt/Mainz: kriegen sich noch nicht zusammengerauft. Dürfen wir noch hoffen?

Chaos Family

Bielefeld: FoeBud e.V., Treff jeden Dienstag um 19:30 im Cafe Durst in der Heeperstr. 64. Monatliche „Public Domain" Veranstaltung, siehe Mailbox. Briefpost: Foebud e.V., Marktstr. 18, D-33602 Bielefeld, Fax. (0521) 61172, Mailbox (0521) 68000 und Telefon-Hotline (0521) 175254 Mo-Fr 17-19 Uhr. EMail zentrale@bionic.zerberus.de

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

Österreich: Public Netbase, http://www.t0.or.at/

Engagierte ComputerexpertInnen, Postfach 168, A-1015 Wien.

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

Editorial

Liebe Zielgruppe,

Situation Normal – All Fucked Up?

Der diskordische Lebenswandel ist manchmal ganz schön schlecht für die Gesundheit. Der Congress ist gerade vorbei, da wälzt man sich auf die andere Seite und schon steht die CeBIT vor der Tür. Also wieder volles Chaosprogramm: Der Club ist nun zum zweiten Mal mit einem eigenen Stand vertreten und wird wieder einen „kleinen Congress“ durchführen – tägliche Workshops zu den aktuellen Themen.

Das letzte Vierteljahr war erfreulich ereignisreich. Der Berliner Erfa-Kreis hat sich neue Clubräume gesucht und auch die Kölner haben ihren Erfa-Kreis gestartet und ihn mit einer Party eingeweiht. Bei den Berlinern findet mit dem „Club Discordia“ zusätzlich noch ein regelmäßiger, öffentlicher Donnerstags-Treff statt. Und das Chaosradio hat mittlerweile seine 25. Sendung über den Äther gejagt. Na bitte.

[Beginn Werbeblock] Dank des Internet Service Providers SNAFU (a.k.a. Interactive Networx) konnte nicht nur der letzte Congress problemlos mit Internet bestückt werden, nun ist auch unser Web Server direkt an einer Datenautobahnzufahrt geparkt und kann endlich mit der benötigten und gewünschten Bandbreite dem Ansturm der Klickenden entgegentreten.

Da sich die Zusammenarbeit mit SNAFU dabei stets extrem unkompliziert gestaltet hat, bedanken wir uns auch schön artig und knallen dafür auch das SNAFU-Logo fett auf diese Seite – für Pyramiden haben wir ja ‘eh ne Schwäche **[Ende Werbeblock]**.

Diese Datenschleuder bringt die aktuelle Themenlage vor allem durch einen Rückblick auf Veranstaltungen des letzten Congresses auf den Tisch. Der Kampf um die Freiheit der Privatsphäre scheint erst richtig loszugehen (lausch, lausch) und der nicht abreißende Trend in Richtung Totalvernetzung und Globalisierung wirft auch schon seine Schatten voraus. Eine Betrachtung der Sicherheitskonzepte der diesen Systemen zugrunde meist zugrundeliegenden Software findet Ihr auch in diesem Heft. Apropos Sicherheit. Die ist übrigens berechenbar! Das ist doch mal was neues. Den Beleg dafür findet Ihr auch auf den nächsten Seiten. Übrigens: wer in Zukunft prima Artikel für die Datenschleuder schreibt, wird mit einem Abo belohnt!

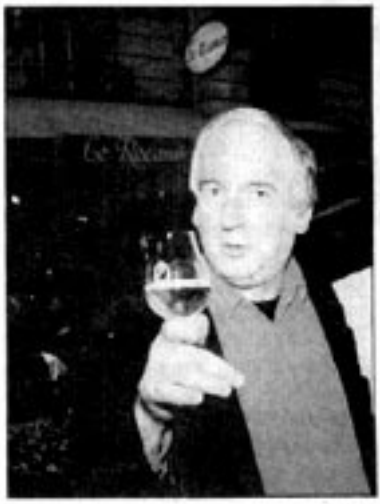
Viel Spaß am Gerät!
tim@ccc.de

Index

Let's pie! Let's pie!

Until last week, Noel Godin was relatively unknown in the United States. A 52-year-old Belgian author, film historian, actor („The Sexual Life of the Belgians"), writer („Cream and Punishment") and „entarteur" (a Godin coinage that roughly translates as „encaker" or „pie-er"), Godin led the gang that gave to Bill Gates what so many of us only dream of: a big wet pie in the face. The attack took place at the entrance of Le Concert Noble on Arlon Street in Brussels and was widely reported in the press.

Godin doesn't own a computer and didn't even know what a URL is. His girlfriend, however, uses a PC. (This interview was conducted and translated by Hugues Henry.)



Prestige

Pie-throwing anarchist Noel Godin of Brussels toasts his work.

Who are you, Noel Godin?
I'm part of a gang of bad hellions that have declared the pie war on all the unpleasant celebrities in every kind of domain (slogan: „Let's pie! Let's pie! Nincompoop guys!"). We began to act against „empty" celebrities from the artistic world who were thinking they were the cat's whiskers. Then we attacked the TV news business in France, for instance, Patrick Poivre D'Arvor [a famous French TV presenter]. Then it became political with Philippe Douste-Blazy in Cannes, the French minister of culture, or the other French minister Nicolas Sarkozy last year in Brussels.
When did you first pie someone?
In November 1969, with French writer Marguerite Duras, who represented for us the „empty" novel.
Why did you choose Bill Gates?
Because in a way he is the master of the world, and then because he's offering his intelligence, his sharpened imagination and his power to the governments and to the world as it is today — that is to say gloomy, unjust and nauseating. He could have been a utopist, but he prefers being the lackey of the establishment. His power is effective and bigger than that of the leaders of the governments, who are only many-colored servants. So Bill Gates was at the top of our lists of victims. The attack against him is symbolic, it's against hierarchical power itself. Our war cry was explicit: „Let's pie! Let's pie the polluting lolly!"
So you have a whole list of people you want to pie?
Yes, we have meetings here in my house. These are funny meetings; we have a good time with good drinks and at the same time we plot. We always agree on the target choice and then we have to study how to reach the target.
How did you prepare to pie Bill Gates?
For several years, there's been a new phenomenon. Traitors appear in the entourage of our victims who contact us to give us firsthand information. Our victims, at first sight, are very unpleasant and they are far from being loved in their own circle; this is our trump. For instance, these last years, Patrick Poivre D'Arvor, [producer] Daniel Toscan du Plantier and [French minister] Nicolas Sarkozy have been betrayed. In the case of Bill Gates, a member of the staff of Microsoft Belgium contacted us and gave us a mysterious rendezvous. Thanks to him, the operation was a success. Of course we won't give his name. It's a secret; only a few know his identity. But we want to tell it because we would be very amused if there was suspicion in the staff of Microsoft. „Who's the traitor?!"

It happened one week before the arrival of Bill Gates in Belgium. We received, little by little, very precise information about the planning of the Bill. Some Parisian accomplices followed him the day before, step by step, notably when he first met Lionel Jospin [French prime minister]. For instance, we learned that he was always escorted by five armed bodyguards but no more. In Belgium, he had four motorcycle policemen and

Nincompoop guys!

he had five important rendezvous that day. So, to succeed, we only had one solution: our number. We were 30 individuals. That's why we succeeded. We were extremely determined, we were in a good mood. We were a funny commando.

We were divided in „gloupinesques" [from his pseudonym, Le Gloupier] fighting units of three on Arlon Street, where people were waiting for him in Le Concert Noble. There was traffic in the street so the plotters were anonymous. When Bill Gates arrived with screaming sirens, he walked outside his car and as he was climbing the steps several of our fighting units gathered and they created a kind of pie whirl that fell on him. The bodyguards were completely distraught. None of them even took out his gun. They were as dazed as Bill was.

Do you know why there's a traitor in the staff of Microsoft Belgium? What were his motivations?

This man told us he really loved Bill Gates in the past, saying that he was very cool and passionate. But little by little he considered that his power had tainted him, and that he was becoming more and more haughty with his own collaborators. So the man who gave us the information considered, and he's not alone, that it wouldn't be bad to teach Bill a lesson, to bring him back to reality.

That's how he explained to us why he was doing it. He's far from being a member of our band, he's not an anarchist and he likes his work with Microsoft, but he thought it had to happen.

So you weren't paid by someone from Netscape or Oracle?

Certainly not; I wasn't even aware of their existence.

Weren't you afraid of the armed bodyguards and the police?

This time, yes, we were afraid. We didn't sleep very well the night before. We thought, since the bodyguards of Bill Gates are professional, they won't fire. I told my men, „Be happy and show it is only cream." To be strong, we drank some good Trappist beers. So they were laughing and joking when they went to the front... Of course I wasn't in the commando because the authorities, the press... they know my face. It would have been a mistake, even with a disguise. So I was on an adjacent street.

How many pies were thrown?

Four touched Bill Gates in the face. There were 25 pies in all. One of the secrets of the gloupinesque operation is that you don't have to throw the pies. You must put the pies point-blank in the face of the victim. One of the members of the victorious commando is the filmmaker Rémy Belvaux („Man Bites Dog"). He unfortunately lost his papers and so the cops revealed his identity.

What were their feelings just the second after they touched Bill Gates with the pie?

The exhilaration of victory. Exquisite pleasure. The gloupinesque operations have a 95 percent success rate. But each time we are stressed, and each time it's the same pleasure.

How did Bill Gates react?

…Tortenwerferterroristeninterview

He had a kind of promotional smile that became a kind of smile made of sand...

When you touch your victim, don't you have the feeling of being powerful? You had pies, but it could have been a knife.

Yes, but this is not our problem. We are comical terrorists and the pie is symbolic. The victim is only injured in his self-esteem. We take a lot of care that the pies can't hurt psysically. The pastry is soft and full of cream.

Do you cook the pies?

No, we are very lazy. We buy the pies in a shop nearby the place of the crime. This time, the pies where coming from a little shop called Au Petit Pain Frais, chaussée de Haecht.

Will Bill Gates pursue your commandos?

No, it would be catastrophic for him and his reputation.

If someone gave you money to pie his enemy, would you accept it?

We have never been pie mercenaries. But we've had several offers of a good amount of money. For instance, I had an offer to pie Catherine Deneuve in Cannes and also Sharon Stone. I refused. I love Catherine Deneuve and the movies of Jacques Demy; and that year Sharon Stone was in a western I really liked. So I had nothing against her. We are pie pirates. But if we receive money when we pie someone, we are not puritan leftists. We received money once: in the case of [famous French singer and actor] Patrick Bruel. We offered the money to the anarchist Parisian magazine Mordicus. So if someone wants to give us money we won't misuse it. I could really enjoy life if I could earn much money doing this job! It's a big game and we have fun together. We want to live fast and to laugh as much as we can. We want to transform our lives just like Oscar Wilde wanted to. Everything is awful around us, so let's try to have fun.

If Bill Gates had to come back in a few months in Belgium, would pie him again?

We shall see. But we declare war on all the governments of the world, on Tony Blair, on Bill Clinton, on the pope... When the pope last came to Belgium, if we'd had a traitor sponsoring us, we'd have pied him. We had a strategy. For us, the pope is a dangerous serial killer because he is against the preservative [birth control]. On our blacklist, you will also find Demi Moore; Tom Cruise and John Travolta, who are both members of the Scientology; Bill Graham... On the other hand, we have more and more sympathizers everywhere. We had thousands of propositions to help us, even abroad. We also have many enemies. But we are like the characters of a cartoon. We are like Laurel & Hardy, Bugs Bunny, the Marx Brothers, the yippies of May 1968.

The Netly News
http://cgi.pathfinder.com/netly/0,1039,1733,00.html
Interview by Hugues Henry February 9, 1998

Krypto-War und PGP-Verkauf

Auf dem Chaos Communication Congress 1997 haben wir eine intensive und mitunter erhitzte Debatte über die Kryptoregulierung, ihre deutsche Variante und die vermeintlichen Hintergründe geführt. Der eigentlich zur Podiumsdiskussion geladene und maßgeblich für eine Regulierung von Kryptographie (Verbot aller Verfahren, wo der Schlüssel nicht hinterlegt ist bzw. so kurz ist, daß staatliche Stellen mitlesen können) eintretende Ministerialdirektor des Innenministeriums Reinhard Rupprecht hatte kurz vor dem Kongress leider abgesagt.

Dies führte zu einer eher heftig geführten Podiumsdiskussion „Wirtschaftsspionage und Innere Sicherheit“, die letztlich auch die eher mittelrelevante Frage aufstellte, warum sich eigentlich das deutsche Innenministerium so kompatibel zu den amerikanischen Plänen eines globalen Key-Escrow verhält. Inwieweit die deutsche Regierung dabei „ferngesteuert“ von amerikanischen Stellen ist, sei dahingestellt.

Mittlerweile ist jedenfalls klar, daß die öffentliche Stille des Innenministeriums nichts Gutes zu verheißen hat. Es ist nicht etwa so, daß Innenminister Kanther seine Vorstellungen nach dem eher heftigen Protest – auch aus Kreisen der Industrie – fallengelassen hat. Vielmehr versucht das Innenministerium derzeit über das BSI in einem ETSI „Policy“ Gremium auf der Ebene der europäischen Normungen – der de-facto-Standards - dafür zu sorgen, daß hier entsprechende Regulierungen implementiert werden. Ein solches Verhalten des deutschen Innenministers muß nicht unbedingt – das ist durchaus plausibel – auf Druck amerikanischer Stellen bzw. des Außenministeriums herrühren. Der Kanther’sche Überwachungswahn könnte sich auch durchaus die amerikanischen Vorstellungen zu eigen gemacht haben. In den Auswirkungen kann uns das aber auch ziemlich egal sein – mit Überzeugungstätern haben wir es in der Debatte zwar nicht durchgehend, aber doch in zunehmendem Maße zu tun.

Insofern scheinen mir zunächst andere Fakten wichtiger. Anlaß zur Sorge bietet die Entwicklung um PGP. Nachdem Phil Zimmermann unter Beibehaltung gewisser Entscheidungshoheiten seine Firma PGP Inc. an die Firma Network Associates (NETA) verkauft hat, ist die weitere Entwicklung unübersichtlich geworden. NETA war nach dem Kauf zunächst aus der Key Recovery Alliance (`http://www.kra.org`) ausgetreten. Die „Key Recovery Alliance“ ist dabei ein Zusammenschluß von Firmen, die die Vorstellungen der amerikanischen Regierung unterstützen und im vorauseilenden Gehorsam Key Recovery unterstützen. Dies klingt vielleicht etwas unglaublich, ist aber nur logisch, wenn man dazu weiß, daß nur Firmen, die Key Recovery unterstützen, in diesem Technologiebereich noch Aufträge der amerikanischen Regierung bekommen. Auch die deutsche (!) Siemens AG ist beispielsweise Mitglied der KRA.

Nachdem NETA vor kurzem die Firma Trusted Information Systems (TIS) gekauft hat, erwägt sie nun der KRA wieder beizutreten (Quelle: `http://www.news.com/News/Item/0,4,19402,00.html`). Der Hintergrund erscheint wiederum aus geschäftlicher Sicht logisch. Der Geschäftsführer von TIS ist eine der treibenden Kräfte der KRA, das Kerngeschäft der Firma die Belieferung von Regierungsstellen. Wenn man die KRA-Mitgliedschaft von TIS durch den Kauf beenden würde, würde man automatisch auch einen Großteil der Kunden verlieren:

> *„It’s highly likely that Network Associates will be a member,“ Network Associates chief executive Bill Larson said today. „The Key Recovery Alliance is a very important organization... Philosophically, we are bridging two discrete worlds – the PGP-Internet world and the TIS intelligence world.“ TIS has major consulting contracts with U.S. government agencies.*

Das sieht – mit Verlaub – ziemlich Scheiße für die Zukunft aus. Am besten wir gewöhnen uns gar nicht erst an die Oberfläche von PGP 5, sondern rufen lieber nach Programmierern, die anständige 2.6.2 Implementationen oder Alternativen liefern. Aufpassen!

andy@ccc.de

Im Fadenkreuz: SAP R/3

Einer unser Autoren hatte vor einigen Monaten das Glück (oder sagen wir angesichts des geringen Unterhaltungsfaktors besser: die Gelegenheit) eine Administrator-Schulung für SAP R/3 zu besuchen. Untenstehend geben wir seine Notizen, subjektiven Anmerkungen und persönlichen Bemerkungen wieder, damit der geneigte Leser einen ersten Eindruck von den Zuständen in einem System bekommt, mit dem 80% der Buchhaltung der deutschen Wirtschaft betrieben wird.

Konzeptionelle Features von R/3:

1. Drei-Schichten-Modell
   Die SAP unterscheidet logisch zwischen Datenbank, Applikation und Präsentation.R/3 ist prinzipiell ein Interpreter mit einer 4GL-Sprache namens ABAP/4.
2. Der Datenbankserver ist ein traditioneller SQL-Server wie Oracle. Es gibt aus der Sicht von R/3 immer genau einen zentralen Datenbankserver. Es gibt verteilte Datenbankserver, die aber nur auf Datenbankebene verteilt werden, d.h. für SAP sehen sie immer noch wie eine Datenbank aus.
3. Die Application-Server interpretieren die ABAP-Programme und machen die Datenbankzugriffe.Die Prozesse müssen nicht auf dem gleichen Rechner wie die Datenbank laufen, sie müssen nicht mal untereinander auf der gleichen Hardware laufen.
4. Die Präsentation wird von einem speziellen Terminal-Programm namens SAPGUI erledigt. Der Traffic zwischen GUI und Application Server ist Low-Volume und auch für WAN-Verbindungen gedacht und so stellt sich die SAP auch eine Verteilung vor.
5. Alle Daten liegen in der Datenbank.Auch die ABAP-Programme und die Konfigurationsdateien. R/3 kommt mit über 10.000 Tabellen.
6. Wilkürliche Limits wo man hinguckt.Welche davon historisch bedingt sind, welche technisch, welche inzwischen nicht mehr nötig wären, …?

SAP wirbt gerne mit dem Schlagwort „Sicherheit“ für R/3. Leider ist damit nicht die Sicherheit vor mutwilligen Angriffen gemeint, sondern vor versehentlichem Datenverlust, z.B. durch Plattenausfall.In der Tat geht R/3 in puncto Ausfallsicherheit ziemlich weit. Dieser Aspekt von R/3 soll hier aber nicht unser Thema sein.

Für eine Security-Prüfung von R/3 muß man sich natürlich zuerst fragen, welches Ziel ein Angriff haben könnte. Bei R/3 ist die Angriffsfläche natürlich besonders hoch, weil R/3 potentiell sehr sensible Daten beinhaltet, wie z.B. Gehälter, Rechnungen, Lagerbestände, Produktionszahlen oder Personaldaten. Wir definieren also als höchstes Ziel für einen Angreifer den Zugriff auf R/3-Tabellen. Besondere Beachtung verdient hierbei der Umstand, daß mehr als 80% aller Angriffe auf Computersysteme von sogenannten Innentätern, also frustrierten oder abgeworbenen Mitarbeitern begangen werden.

Das erste Thema ist also das Berechtigungskonzept von R/3. Da bei R/3 die Daten nicht direkt im Filesystem abgelegt sind, sondern in Datenbank-Tabellen, übernimmt die User-Überprüfung nicht das Betriebssystem. Das ist einerseits erfreulich, weil man dann auf OS-Ebene den R/3-Usern keine Accounts einrichten muß. Andererseits ist das bedenklich, weil auf Betriebssystem-Ebene die Zugriffssicherung ein gut verstandenes Problem ist.

Die offensichtliche Alternative für die Rechte-Prüfung wäre, auf Datenbank-Ebene den Zugriff zu regulieren. Die SAP entschied sich aber dafür, die Zugriffsberechtigungen komplett selber zu implementieren. Auf Nachfrage wurde als Begründung genannt, daß die Datenbanken das alle unterschiedlich machten und man ja portabel

bleiben wolle. Seltsam, wo es doch sowieso für jedes Datenbank-Backend eigenen Code gibt.

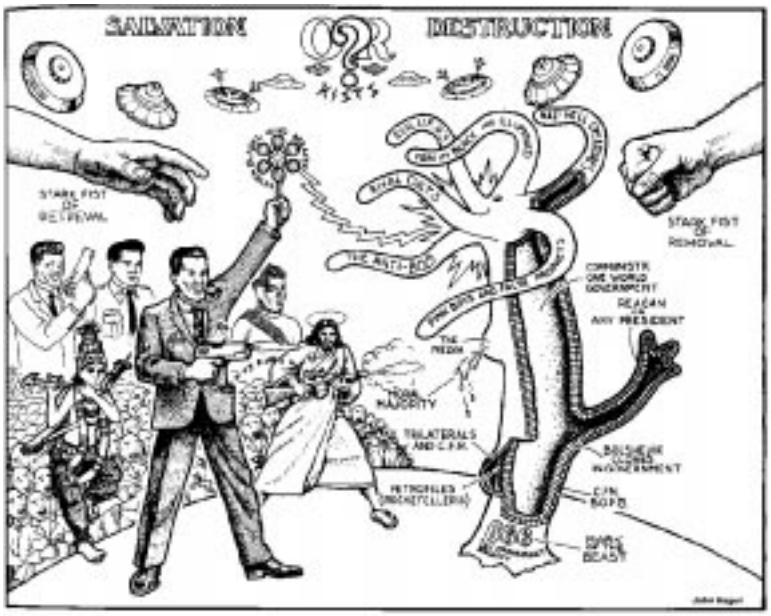
An dieser Stelle freut sich der Sicherheits-Fachmann, daß bei R/3 die ABAP-Quellen mitgeliefert werden. Man kann sich also anschauen, wie die Berechtigungen implementiert werden. Und ein erster Blick sieht vielversprechend aus, hat sich die SAP doch entschieden, die Rechte rein kumulativ zu vergeben, d.h. was nicht explizit erlaubt wurde, ist verboten.

Leider stellt sich heraus, daß die Rechte nicht pro Datenbank-Objekt vergeben werden, sondern die ABAP-Programme „von Hand“ (und nur von Hand!) die Berechtigungen prüfen. Wünschenswert wäre gewesen, einem User den Lesezugriff auf die Gehalts-Tabelle zu verweigern, und dann sicher zu sein, daß er keinen Zugriff hat. Bei R/3 muß man alle zugreifenden Programme daraufhin untersuchen, ob sie dem User Zugriffe ermöglichen, die er nicht haben dürfte. Bei einem Tabellenumfang von über 50 MB bei den ABAP-Quellen ist das sicher keine triviale Aufgabe.

Schlimmer noch: das eherne Prinzip der Sicherheit ist so verletzt, das Prinzip der minimalen Berechtigung! Es ist nicht möglich, einem Developer Zugriff nur auf seinen Bereich einzuräumen. Wenn eine Firma jetzt einen Consultant einstellt, der für sie ein ABAP-Programm schreibt, und der Mann fühlt sich schlecht behandelt, kann er in seinem kleinen Buchungs-Programm auch vollen Zugriff auf die User- und Payroll-Tabellen nehmen oder gar das ganze System zum Stillstand bringen. Wünschenswert wäre ein zweistufiges Sicherheitsmodell, wo für jedes Programm genau wie für jeden User explizit der Zugriff erlaubt werden muß.

Der einzige Schutz gegen maliziöse Programme ist die sogenannte System-Landschaft. Eine R/3-Installation besteht gewöhnlich aus mehreren Systemen. SAP empfiehlt drei Systeme: ein Development-System, ein Quality-Assurance-System und ein Production-System. Die Idee ist, daß der Developer mit seinem Programm nur auf dem Development-System spielen darf, und das Programm dann nur vom Administrator zum jeweils nächsten System transportiert werden kann. Das mag zwar gegen versehentlichen Datenausfall helfen, aber gegen Datums- oder System-ID-Trigger ist so kein Kraut gewachsen.

Halten wir also fest: jeder Entwickler kann eine R/3-Installation kompromittieren. Prinzipiell kann der Administrator natürlich alle entwickelten Programme nach offensichtlichen trojanischen Code-Fetzen absuchen, aber das ist nicht zumutbar und auch keine prinzipielle Lösung für das Problem.



Um die Tragweite dieses Problems zu begreifen, muß man einen Blick in den Stellenmarkt einer fast beliebigen IT-Publikation werfen und mit Erstaunen feststellen, daß praktisch alle Firmen händeringend R/3-Experten suchen. Der Markt konnte dem explosiven Wachstum der SAP nicht folgen. Es wäre also ein leichtes für eine Firma (oder einen Nachrichtendienst), der Kon-

kurrenz einen SAP-Consultant unterzuschieben, mit dem Ziel, Intelligence zu sammeln oder einen Bankrott zu erzeugen (Backups werden sicher nicht ewig aufgehoben und ein trojanisches Pferd mit Datumssteuerung muß nur den Backup-Zyklus überleben, um auf allen Backups vorhanden zu sein). Wenn man jetzt bedenkt, daß praktisch alle größeren Unternehmen R/3 einsetzen, ist die strategische Bedeutung einer R/3-Kompromittierung für einen Nachrichtendienst offensichtlich.

Das Problem liegt aber noch tiefer. Wie oben bereits angedeutet, liegen alle ABAP-Quellen in einer Datenbank. Ein direktes Editieren scheidet also aus. Bei R/3 werden ABAP-Quellen mit dem SAPGUI in einer R/3-Transaktion editiert, ähnlich wie man die User-Tabelle bearbeiten würde. Diese Workbench-Transaktion ist genau wie die anderen Transaktionen selber in ABAP geschrieben. Dieser Umstand ermöglicht eine Attacke, gegen die praktisch kein Kraut gewachsen ist. Es ist nämlich denkbar, den ABAP-Quellcode der Workbench-Transaktion so zu ändern, daß es maliziösen Code nicht anzeigt, inklusive dieser Änderung an sich selber natürlich. Das Ergebnis wäre ein R/3-System, das genau aussieht wie immer, und sogar eine Analyse der ABAP-Quellcodes zeigt ein unverändertes System. Tatsächlich könnten im Hintergrund aber praktisch beliebige Datenbank-Modifikationen laufen.

Das klingt möglicherweise nicht oder nur unter gewaltigem Aufwand umsetzbar. Die Geschichte zeigt aber einen ähnlichen (sogar komplizierteren Fall), bei dem nicht mal materielle Gesichtspunkte der Hintergrund waren, nämlich ein C-Compiler, der erkannte, wenn er das Login-Programm übersetzte, und dort einen weiteren Root-Zugang einbaute, aber auch eine Übersetzung von sich selber erkannte und diesen Code wieder einbaute in das Kompilat, so daß alle Quellcodes „sauber“ waren. Wenn man bedenkt, um welche Geldmengen es geht, wenn man einen Angriff wie diesen gegen die deutschen Großbanken oder Automobil-Hersteller richten würde (der Angriff müßte nur einmal entwickelt werden und wäre sofort weltweit einsetzbar!), wird einem das Ausmaß der Problematik bewußt. Weil auch innerhalb von SAP mit der Workbench gearbeitet wird, würden auch die SAP-Entwickler von so einem trojanischen Pferd nichts mitbekommen, und es ab dem nächsten Update mit ausliefern. Daß das nicht schon längst geschehen ist, kann in meinen Augen auch niemand wirklich ausschließen. Vielleicht als Anmerkung am Rande: R/3 übersetzt die ABAP-Quellen in einen Zwischencode, der natürlich auch in einer SQL-Tabelle gespeichert wird. Es würde also wahrscheinlich reichen, diesen kompilierten Zwischencode in der Tabelle zu modifizieren, um den gewünschten Effekt zu haben.

Nach diesen allgemeinen Überlegungen noch ein paar konkrete Betrachtungen: Ein Interpreter-Kernel ist ein sehr gutes Konzept. Er kann ganze Fehlerklassen ausschließen, wie Pufferüberläufe und Memory-Leaks. Aber ein Interpreter macht das Gesamtprogramm nur vertrauenswürdiger, wenn er klein und überschaubar ist. Der R/3-“Kernel“ ist über 11 Megabytes groß (das ist bereits das gestrippte Binary!).

Insgesamt heißt Security auch Schutz gegen Denial-Of-Service-Attacken, d. h. es darf nicht möglich sein, ein System durch einen Bug zum Komplett-Absturz zu bringen. Bekanntermaßen steigt die Wahrscheinlichkeit für die Existenz

eines Bugs exponentiell mit der Programmgröße. Bei einem 11-MB-Kernel und 50 MB ABAP-Quellen kann von Überschaubarkeit bei R/3 keine Rede sein. Die Software-Industrie hat sich in den letzten Jahrzehnten Konzepte überlegt, um ein Projekt überschaubar und wartbar zu halten. An erster Stelle steht, daß der Code kommentiert sein muß und daß Bezeichner aussagekräftig vergeben werden. Bei R/3 scheinen Bezeichner auf 10 Zeichen beschränkt zu sein, so daß Bezeichner grundsätzlich Namen wie Line Noise haben. Ähnlich sieht es bei den Namen von Tabellen und Tablespaces aus. So erkennt man den R/3-Newbie daran, daß er noch nicht weiß, wofür PSAPBTABD steht. (Das ist der Datenteil (im Gegensatz zum Index-Teil, der PSAPBTABI heißt) der Bewegungsdaten-Tabelle (d.h. Buchungen). Der Wartbarkeit ist das natürlich extrem abträglich. Hinzu kommt, daß innerhalb von R/3 sehr oft Code dupliziert wird, der von anderen (gewöhnlich besser) erledigt wird. U. a. handelt es sich um:

- Userverwaltung
- Editor für ABAP-Programmierung (edlin-Niveau)
- Versionsverwaltung (kein Undo außer über Datenbank-Backups)
- Scheduler (deutlich weniger leistungsfähig als cron)
- Backup
- Drucken (für Remote-Drucken zu NT haben sie ein SAPLPD. EXE geschrieben)
- OS-Monitor (sammelt Statistiken über das System)

Schließlich sorgen bei R/3 noch Details für einen bitteren Nachgeschmack wie die Limitierung von Passwörtern auf 8 Zeichen, wobei Groß- und Kleinschreibung egal ist. Die Erfahrung sagt außerdem, daß SAP-Installationen gewöhnlich von Nicht-Profis gemacht werden. Meistens wird für die Installation und das Customizing ein Consultant eingestellt, der danach aber weg ist. Und R/3-Profis haben selten gleichzeitig ein tieferes Verständnis für das zugrundeliegende Betriebssystem. So ist in praktisch allen Fällen auf den R/3-Servern noch jeder Standard-Dienst des Betriebssystems und der Datenbank aktiviert, ja telnet und ftp werden sogar ständig noch benutzt (telnet zur Fernwartung und ftp weil die eingebauten Methoden zur Dateiübertragung zu langsam sind). Schlimmer noch — SAP setzt eine NFS-Installation zwischen den Systemen voraus! Aber auch alte Bekannte wie rexec werden von R/3 benutzt.

Wem diese Probleme noch nicht reichen: die eigentlichen Transaktionen zwischen R/3 und dem SAPGUI werden nicht verschlüsselt. Sie gehen zwar nicht im Klartext über das Netz, weil sie komprimiert sind, aber von Sicherheit kann auch hier nicht die Rede sein. Wenigstens stehen die Passwörter nicht im Klartext in der Datenbank…

Sozusagen als Salz in der Suppe bietet SAP jetzt auch einen Internet Transaction Server an, der den Web-Server mit dem Warenwirtschafts-System verbinden soll. Dieser Server wird nur für NT angeboten.

...SAP R/3

Um es auf den Punkt zu bringen: R/3 ist unsicher. Betriebssysteme sind meistens auch unsicher. Sobald jemand Shell-Zugriff auf einem System hat, hat er gewöhnlich auch schnell Zugriff auf die Oracle-Datenbank, und damit hat er Total-Zugriff auf die R/3-Datenbasis. In diesem Moment hat der Systembetreiber verloren. Andersherum kann ein Developer in einem R/3-System die Datenbank komplett ändern und auch beliebige Shell-Kommandos ausführen, d. h. sich eine Shell erzeugen.

Neben den üblichen netzwerkbezogenen Sicherheitsmaßnahmen bleibt also für den Systembetreiber eigentlich nur:

- Auf keinen Fall Windows NT einsetzen! Schon gar nicht als Server.
- Zu hoffen, daß keine trojanischen Pferde in der Datenbasis sind
- Darauf achten, daß die Consultant-Firma haftbar und gut versichert ist

Die Account-Daten in einer SAP R/3-Standardinstallation sind:

- Es gibt einen Client 066, genannt „Early Watch“, mit dem die SAP das gleichnamige Support-Programm fahren kann, d.h. sie gucken sich dann remote die Installation an und sagen, ob sie „gut“ ist. Passwort ist „support“. „Client“ steht bei SAP nicht für User, sondern für einen Parameter beim Datenbankzugriff. Normalerweise braucht man eigentlich nur einen Client, aber wenn man möchte, kann man auch einen weiteren Client haben, der alle Daten extra herumliegen hat (obwohl physikalisch in der gleichen Datenbank). Mit dem Extra-Client kann man sich also theoretisch nur die clientunabhängigen Daten anschauen (das sind so Sachen wie „in welchem Tablespace liegt welche Tabelle“).
- Auf Oracle-Ebene:

```
User       Passwort
SYS        CHANGE_ON_INSTALL
SYSTEM     MANAGER
SAPR3           SAP
```

- Auf R/3-Ebene:

```
User       Passwort
DDIC       19920706
SAP*       06071992
```

(6.7.1992 war das Datum der ersten R/3 Produktiv-Installation)

- Passwörter auf Systemebene werden bei der Installation abgefragt.

anonymous@some.where

Nokia Security Code Generator

Das Programm berechnet aus der 15-stelligen IMEI (International Mobile Equipment Identifier) den werksseitig eingestellten Sicherheitscode von Nokia-Mobiltelefonen. Wenn bei einem Nokia-Telefon die Sicherheitsstufe „Telefon“ ausgewählt ist, kann man ohne den Sicheheitscode keine andere SIM-Karte benutzen.

Der Algorithmus kann den Sicherheitscode für alle Geräte der Serien NHB, NHE und NHK berechnen, d.h. für entsprechende 20**, 21**, 31**, 38** und 81**. Das funktioniert natürlich nur, wenn der werksseitig eingestellte Code nicht geändert wurde. Ansonsten benötigt man den 10stelligen Mastercode, der übrigens ebenfalls aus der IMEI berechnet wird und nicht änderbar ist.

Die IMEI kann man bei Nokia-Telefonen (und den meisten anderen GSM-Telefonen auch) mit *#06# abfragen. Außerdem steht sie in den meisten Fällen auf dem Etikett auf der Rückseite unter dem Akku.

tobias@ccc.de
Source Code von andreas@ccc.de

```
/*
 * security_code.c
 */

unsigned char data_1[] =
{ 0x17,0x2D,0x25,0x29,0x17,0x2D,0x11,0x20,0x12,0x27,0x0E,0x23,0x1B,0x0B,0x27 };
unsigned char data_2[] = { 2,6,9,4,9 };
unsigned char data_3[5][15] = {
{ 0x17,0x2C,0x43,0x0E,0x22,0x13,0x43,0x4D,0x59,0x16,0x22,0x4E,0x37,0x58,0x5C },
{ 0x4B,0x2D,0x5A,0x12,0x24,0x43,0x35,0x4A,0x47,0x36,0x13,0x17,0x53,0x24,0x13 },
{ 0x22,0x47,0x1D,0x4E,0x62,0x22,0x41,0x17,0x26,0x30,0x2C,0x57,0x38,0x36,0x12 },
{ 0x42,0x2E,0x18,0x2D,0x4E,0x20,0x0E,0x23,0x4A,0x60,0x47,0x25,0x30,0x39,0x3F },
{ 0x21,0x24,0x19,0x13,0x1A,0x25,0x1F,0x36,0x4F,0x20,0x2E,0x43,0x36,0x21,0x15 }
};
unsigned char data_4[] = { 1, 5, 7, 6, 3 };

int security_code(char* imei, char* sec_code) {
  int i,j;
  unsigned char k;
  char local_1[15];

  if(strlen(imei) != 15)
    return 0;
  for(i = 0; i < 15; i++) {
     local_1[i] = imei[i] - data_1[i];
  }
  for(i = 0; i < 5; i++) {
    k = 0;
    for(j = 0; j < 15; j++) {
      k += (local_1[j] ^ local_1[(j + data_2[i]) % 15]) * data_3[i][j];
    }
    k = (k + data_4[i]) % 10;
    sec_code[i] = k + 0x30;
  }
  return 1;
}

main(int argc, char** argv) {
  char sec_code[6];

  security_code(argv[1], sec_code);
  sec_code[5] = 0;
  printf("%s\n", sec_code);
}
```


Lauschangriff: Mit JA stimmten...

Aus dem Plenarprotokoll der 214. Sitzung des Deutschen Bundestages vom 16.1.1998

CDU/CSU: Ulrich Adam, Peter Altmaier, Anneliese Augustin, Jürgen Augustinowitz, Dietrich Austermann, Heinz-Günter Bargfrede, Franz Peter Basten, Dr. Wolf Bauer, Brigitte Baumeister, Meinrad Belle, Dr. Sabine Bergmann-Pohl, Hans-Dirk Bierling, Dr. Joseph-Theodor Blank, Renate Blank, Dr. Heribert Blens, Peter Bleser, Dr. Norbert Blüm, Friedrich Bohl, Dr. Maria Böhmer, Jochen Borchert, Wolfgang Börnsen (Bönstrup), Wolfgang Bosbach, Dr. Wolfgang Bötsch, Klaus Brähmig, Rudolf Braun (Auerbach), Paul Breuer, Monika Brudlewsky, Georg Brunnhuber, Klaus Bühler (Bruchsal), Hartmut Büttner (Schönebeck), Dankward Buwitt, Manfred Carstens (Emstek), Peter Harry Carstensen (Nordst), Wolfgang Dehnel, Hubert Deittert, Albert Deß, Renate Diemers, Wilhelm Dietzel, Werner Dörflinger, Hansjürgen Doss, Dr. Alfred Dregger, Maria Eichhorn, Wolfgang Engelmann, Rainer Eppelmann, Heinz Dieter Eßmann, Horst Eylmann, Anke Eymer, Ilse Falk, Jochen Feilcke, Ulf Fink, Dirk Fischer (Hamburg), Leni Fischer (Unna), Klaus Francke (Hamburg), Herbert Frankenhauser, Dr. Gerhard Friedrich, Erich G. Fritz, Hans-Joachim Fuchtel, Michaela Geiger, Norbert Geis, Dr. Heiner Geißler, Michael Glos, Wilma Glücklich, Dr. Reinhard Göhner, Peter Götz, Dr. Wolfgang Götzer, Joachim Gres, Kurt-Dieter Grill, Wolfgang Gröbl, Hermann Gröhe, Claus-Peter Grotz, Manfred Grund, Horst Günther (Duisburg), Carl-Detlev Freiherr von Hamm, Gottfried Haschke (Großhenner), Gerda Hasselfeldt, Otto Hauser (Esslingen), Hansgeorg Hauser (Rednitzhemb), Klaus-Jürgen Hedrich, Helmut Heiderich, Manfred Heise, Detlef Helling, Dr. Renate Hellwig, Ernst Hinsken, Peter Hintze, Josef Hollerith, Elke Holzapfel, Dr. Karl-Heinz Hornhues, Siegfried Hornung, Joachim Hörster, Hubert Hüppe, Peter Jacoby, Susanne Jaffke, Georg Janovsky, Helmut Jawurek, Dr. Dionys Jobst, Dr.-Ing. Rainer Jork, Michael Jung (Limburg), Ulrich Junghanns, Dr. Egon Jüttner, Dr. Harald Kahl, Bartholomäus Kalb, Steffen Kampeter, Dr.-Ing. Dietmar Kansy, Manfred Kanther, Irmgard Karwatzki, Volker Kauder, Peter Keller, Eckart von Klaeden, Dr. Bernd Klaußner, Ulrich Klinkert, Dr. Helmut Kohl, Hans-Ulrich Köhler (Hainspitz), Manfred Kolbe, Norbert Königshofen, Eva-Maria Kors, Hartmut Koschyk, Manfred Koslowski, Thomas Kossendey, Rudolf Kraus, Wolfgang Krause (Dessau), Andreas Krautscheid, Arnulf Kriedner, Heinz-Jürgen Kronberg, Dr.-Ing. Paul Krüger, Reiner Krziskewitz, Dr. Hermann Kues, Werner Kuhn, Dr. Karl A. Lamers (Heidelberg), Karl Lamers, Dr. Norbert Lammert, Helmut Lamp, Armin Laschet, Herbert Lattmann, Dr. Paul Laufs, Karl Josef Laumann, Vera Lengsfeld, Werner Lensing, Christian Lenzer, Peter Letzgus, Editha Limbach, Walter Link (Diepholz), Eduard Lintner, Dr. Klaus W. Lippold (Offenbach), Dr. Manfred Lischewski, Wolfgang Lohmann (Lüdenscheid), Julius Louven, Sigrun Löwisch, Heinrich Lummer, Dr. Michael Luther, Erich Maaß (Wilhelmshaven), Dr. Dietrich Mahlo, Erwin Marschewski, Günter Marten, Dr. Martin Mayer (Siegertsbrunn), Wolfgang Meckelburg, Rudolf Meinl, Dr. Michael Meister, Dr. Angela Merkel, Friedrich Merz, Rudolf Meyer (Winsen), Hans Michelbach Meinolf Michels, Dr. Gerd Müller, Elmar Müller, (Kirchheim), Engelbert Nelle, Bernd Neumann (Bremen), Johannes Nitsch, Claudia Nolte, Dr. Rolf Olderog, Friedhelm Ost, Eduard Oswald, Norbert Otto (Erfurt), Dr. Gerhard Päselt, Dr. Peter Paziorek, Hans-Wilhelm Pesch, Ulrich Petzold, Anton Pfeifer, Angelika Pfeiffer, Dr. Gero Pfennig, Dr. Friedbert Pflüger, Beatrix Philipp, Dr. Winfried Pinger, Ronald Pofalla, Dr. Hermann Pohler, Ruprecht Polenz, Marlies Pretzlaff, Dr. Albert Probst, Dr. Bernd Protzner, Dieter Pützhofen, Thomas Rachel, Hans Raidel, Dr. Peter Ramsauer, Rolf Rau, Helmut Rauber, Peter Rauen, Otto Regenspurger, Christa Reichard (Dresden), Klaus Dieter, Reichardt (Mannh), Dr. Bertold Reinartz, Erika Reinhardt, Hans-Peter Repnik, Roland Richter, Dr. Norbert Rieder, Dr. Erich Riedl (München), Klaus Riegert, Dr. Heinz Riesenhuber, Franz Romer, Hannelore Rönsch (Wiesbaden), Heinrich-Wilhelm Ronsöhr, Dr. Klaus Rose, Kurt J. Rossmanith, Adolf Roth (Gießen), Norbert Röttgen, Dr. Christian Ruck, Volker Rühe, Dr. Jürgen Rüttgers, Roland Sauer (Stuttgart), Ortrun Schätzle, Dr. Wolfgang Schäuble, Hartmut Schauerte, Heinz Schemken, Karl-Heinz Scherhag, Gerhard Scheu, Norbert Schindler, Dietmar Schlee, Ulrich

Umgang frei nach altem Testament

Die hier genannten Bundestagsabgeordneten haben gemäß altem Testament ihr Grundrecht auf die Unversehrtheit der Wohnung bzw. ihre Privatsphäre eingebüßt. (Vgl. Jesaja 8,10)

Abgesehen davon empfiehlt sich zur angemessenen Bewußtseinserweiterung im Wahljahr 1998 die Lektüre des vollständigen Plenarprotokolls vom 16. Januar 1998 im Bundestag:

`http://www.bundestag.de/ftp/13214c.zip`

Schmalz, Bernd Schmidbauer, Christian Schmidt (Fürth), Dr.-Ing. Joachim Schmidt (Halsbrücke), Andreas Schmidt (Mülheim), Hans-Otto Schmiedeberg, Hans Peter Schmitz (Baesweiler), Michael von Schmude, Birgit Schnieber-Jastram, Dr. Rupert Scholz, Reinhard Freiherr von Schorlemer, Dr. Erika Schuchardt, Wolfgang Schulhoff, Dr. Dieter Schulte (Schwäbisch Gmünd), Gerhard Schulz (Leipzig), Frederick Schulze (Sangerhausen), Diethard Schütze (Berlin), Clemens Schwalbe, Dr. Christian Schwarz-Schilling, Wilhelm Josef Sebastian Horst Seehofer, Marion Seib, Wilfried Seibel, Heinz-Georg Seiffert, Rudolf Seiters, Johannes Selle, Bernd Siebert, Jürgen Sikora, Johannes Singhammer, Bärbel Sothmann, Margarete Späte, Carl-Dieter Spranger, Wolfgang Steiger, Erika Steinbach, Dr. Wolfgang Freiherr von Stetten, Dr. Gerhard Stoltenberg, Andreas Storm, Max Straubinger, Matthäus Strebl, Michael Stübgen, Egon Susset, Dr. Rita Süssmuth, Michael Teiser, Dr. Susanne Tiemann, Dr. Klaus Töpfer, Gottfried Tröger, Dr. Klaus-Dieter Uelhoff, Gunnar Uldall, Wolfgang Vogt (Düren), Dr. Horst Waffenschmidt, Dr. Theodor Waigel, Alois Graf von Waldburg-Zeil, Dr. Jürgen Warnke, Kersten Wetzel, Hans-Otto Wilhelm (Mainz), Gert Willner Bernd, Wilz Willy Wimmer (Neuss), Matthias Wissmann, Dr. Fritz Wittmann, Dagmar Wöhrl, Michael Wonneberger, Elke Wülfing, Peter Kurt Würzbach, Cornelia Yzer, Wolfgang Zeitlmann, Benno Zierer, Wolfgang Zöller

SPD: Gerd Andres, Robert Antretter, Ernst Bahr, Doris Barnett, Wolfgang Behrendt, Hans Berger, Friedhelm Julius Beucher, Tilo Braune, Dr. Eberhard Brecht, Marion Caspers-Merk, Wolf-Michael Catenhusen, Dr. Herta Däubler-Gmelin, Karl Diller, Ludwig Eich, Peter Enders, Annette Faße, Lothar Fischer (Homburg), Iris Follak, Norbert Formanski, Dagmar Freitag, Anke Fuchs (Köln), Arne Fuhrmann, Monika Ganseforth, Uwe Göllner, Günter Graf (Friesoythe), Dieter Grasedieck, Achim Großmann, Hans-Joachim Hacker, Klaus Hagemann, Manfred Hampel, Alfred Hartenbach, Klaus Hasenfratz, Dieter Heistermann, Reinhold Hemker, Rolf Hempelmann, Dr. Barbara Hendricks, Stephan Hilsberg, Gerd Höfer, Jelena Hoffmann (Chemnitz), Erwin Horn, Eike Hovermann, Lothar Ibrügger, Wolfgang Ilte, Renate Jäger, Jann-Peter Janssen, Dr. Uwe Jens Volker Jung (Düsseldorf), Sabine Kaspereit, Susanne Kastner, Hans-Peter Kemper, Walter Kolbow, Fritz Rudolf Körper, Volker Kröning, Thomas Krüger, Dr. Uwe Küster Werner Labsch, Klaus Lennartz, Dr. Elke Leonhard, Klaus Lohmann (Witten), Dieter Maaß (Herne), Winfried Mante, Christoph Matschie, Ingrid Matthäus-Maier, Markus Meckel, Dr. Jürgen Meyer (Ulm), Ursula Mogg, Siegmar Mosdorf, Christian Müller (Zittau), Gerhard Neumann (Gotha), Dr. Rolf Niese, Leyla Onur, Kurt Palis, Dr. Willfried Penner, Dr. Eckhart Pick, Joachim Poß, Margot von Renesse, Reinhold Robbe, Gerhard Rübenkönig, Dieter Schanz, Rudolf Scharping, Bernd Scheelen, Siegfried Scheffler, Horst Schild, Otto Schily, Dieter Schloten, Günter Schluckebier, Wilhelm Schmidt (Salzgitter), Dr. Emil Schnell, Walter Schöler, Ottmar Schreiner, Dr. Mathias Schubert, Richard Schuhmann (Delitzsch), Brigitte Schulte (Hameln), Volkmar Schultz (Köln), Ilse Schumann, Dietmar Schütz (Oldenburg), Ernst Schwanhold, Rolf Schwanitz, Bodo Seidenthal, Johannes Singer, Dr. Cornelie Sonntag-Wolgast, Wieland Sorge, Dr. Dietrich Sperling, Jörg-Otto Spiller, Dr. Peter Struck, Joachim Tappe, Jörg Tauss, Dr. Gerald Thalheim, Wolfgang Thierse, Hans-Eberhard Urbaniak, Siegfried Vergin, Günter Verheugen, Karsten D. Voigt (Frankfurt), Josef Vosen, Hans Georg Wagner, Wolfgang Weiermann, Reinhard Weis (Stendal), Gunter Weißgerber, Jochen Welt, Lydia Westrich, Helmut Wieczorek (Duisburg), Dieter Wiefelspütz, Verena Wohlleben, Dr. Christoph Zöpel, Peter Zumkley.

Grundgesetz Artikel 20
Grundsätze des deutschen Staates:
„(4) Gegen jeden, der es unternimmt, diese Ordnung zu beseitigen, haben alle Deutschen das Recht zum Widerstand, wenn andere Abhilfe nicht möglich ist."

FDP: Ina Albowitz, Dr. Gisela Babel, Günther Bredehorn, Jörg van Essen, Dr. Olaf Feldmann, Paul K. Friedhoff, Horst Friedrich, Rainer Funke, Dr. Wolfgang Gerhardt, Joachim Günther (Plauen), Dr. Karlheinz Guttmacher, Dr. Helmut Haussmann, Ulrich Heinrich, Walter Hirche, Dr. Werner Hoyer, Ulrich Irmer, Dr. Klaus Kinkel, Detlef Kleinert (Hannover), Roland Kohn, Dr. Heinrich L. Kolb, Dr.-Ing. Karl-Hans Laermann, Uwe Lühr, Günther Friedrich Nolting, Dr. Rainer Ortleb, Lisa Peters, Dr. Günter Rexrodt, Helmut Schäfer (Mainz), Cornelia Schmalz-Jacobsen, Dr. Edzard Schmidt-Jortzig, Dr. Hermann Otto Solms, Carl-Ludwig Thiele, Dr. Dieter Thomae, Dr. Wolfgang Weng (Gerlingen), Dr. Guido Westerwelle.

Aus einer Pressemitteilung des Bundesinnenministeriums: „Rede von Bundesinnenminister Manfred Kanther anläßlich der 2./3. Lesung des Gesetzes zur Änderung des Grundgesetzes (Artikel 13 GG) sowie des Gesetzes zur Verbesserung der Organisierten Kriminalität im Deutschen Bundestag."

Quelle: Spiegel 6/98

Chaos Realitäts Dienst: Kurzmeldungen

EU plant Entschlüsselungsverbot

Als Folge des massiven Lobbyings der Pay-TV Industrie liegt in der europäischen Union zur Zeit eine Gesetzesvorlage zur Abstimmung, die nicht nur den Vertrieb illegaler Pay-TV Dekoder unter Strafen stellen soll, sondern auch die Benutzung und - viel schwerwiegender - die Verbreitung „of any private exchange of information about the security properties“. Damit würden etliche Newsgroups, Mailinglists und der freie Informationsaustausch zu Sicherheitsverfahren stark eingeschränkt. Detail auf:
`http://www.cl.cam.ac.uk/~mgk25/ca-law/`

Fernwürgen

(crd/15.01.98) Laut Agenturberichten ärgert ein Funkpirat an der niederländsichen Autobahn A 15 bei Gorkum Kunden und Mitarbeiter eines „Mc Drives“.

Wenn ein Kunde mit seinem Auto vorfährt und über die Sprechanlage seine Bestellung aufgibt, schaltet sich plötzlich der Unbekannte ein. „Er sagt dann zum Beispiel: ‘Nein halt, doch keinen Hamburger, sondern Pommes und ein Milkshake’“, berichtete am Donnerstag einer der Mitarbeiter. „Und der Kunde bekommt dann etwas ganz anderes, als er bestellt hat.“

Der Funker ist nun schon seit über einem Monat aktiv. „Zum Verrücktwerden“, finden die Telefonistinnen, die die Bestellungen entgegennehmen. Wenn sich der Quälgeist nicht durch veränderte Frequenzen für die Sprechanlage abschütteln läßt, will der Betriebsmanager Anzeige erstatten.

crd@ccc.de

Proprietäre Scheiße bei CD-Writern

Phillips und Pioneer Audio-CD-Writer bespielen normalerweise nur (überteuerte) CD-Rohlinge der eigenen Firma. Hier kann man sich jedoch auch günstiger behelfen: Man öffne den Recorder, lege eine CD vom Hersteller ein, warte ein paar Sekunden und suche dann einen Resetknopf im Inneren des Geräts. Nach Druck auf den Resetknopf springt die Schublade auf und der Rohling kann durch einen billigen ersetzt werden. Der CD-Writer behält die Daten des teureren Rohlings gespeichert und macht somit keine Probleme.

(Ohne Gewähr - wir konnten es nicht testen!)

redbaron@ccc.de

DF1 umsonst ?!

Gerüchten aus der Chaos-Voicemailbox zufolge strahlt DF1 eine Kartensperre nur für 5-6 Monate aus. Dies würde bedeuten, wenn man nach ein paar Monaten DF1 mit Gebühr die Karte kündigt und sofort aus dem Decoder (D-box) entfernt, 5-6 Monate im Schrank liegen läßt, und die Karte dann wieder einsetzt, würde man DF1 kostenlos sehen können. Ebenfalls kostenlos kann man alle d-box-Programme mit einer Händlerkarte sehen. Aus diesem Grund sollen in Hamburg bereits mehrere aus nicht verschlossenen (!) Schubladen gestohlen worden sein.

redbaron@ccc.de

Netscape hilfe Microsoft Kunden, den Explorer zu löschen

Laut einer Reuters Meldung vom 18. Dezember bietet Netscape Kunden mit Microsoft-Plattform die Möglichkeit, automatisch Netscape zu installieren und den Microsoft-Internet Explorer zu löschen.

Ob Sie dazu die Active-X Technologie benutzen wollen, wurde nicht bekannt.

Chip-Implantat für britische Bürger

Laut einer Newsbytes Meldung vom 02. Januar 1998 will die britische Regierung in Kürze alle

Bürger mit einer Chipkarte versehen. Die „citizen's smart card" soll als Interface zwischen Bürger und Regierung das Zahlen von Steuern, Versicherung neben Paßfunktion und Einholung von Sozialhilfe erlauben.

Die Idee hinter der „Smart Card" ist laut dem Britischen Minister für öffentlichen Service „is that people will be able to use the card to identify themselves to the various government computers, all of which will be interlinked with each other."

Die in erster Linie aus finanziellen Gründen eingeführte Karte wird zunächst mit einem PIN Code zu benutzen sein und soll später mit biometrischen Merkmalen gekoppelt werden.

Transparenzkriminalität

Laut einer Reuters-Meldung vom 05. Januar 1998 wurde die Japanische Sakura Bank in Tokio kürzlich opfer von „cyber-criminals". Als Folgen gingen 37 ausgesuchte der 20.000 abgesaugten Kundendateien einer Mailinglist zu.

Erpresser stolpert über Echelon-System?!

Ende Januar wurde der „Hamburger Flughafen-erpresser", ein 25jähriger Bankkaufmann zu dreieinhalb Jahren Gefängniss verurteilt. Das Gericht ging von einem minderschweren Fall aus, da er lediglich gedroht habe mit Sprengstoff belandenen ferngesteuernten Modellflugzeugen in die Triebwerke von startenden Maschinen zu fliegen. Der 25jährige hatte gestanden damit insgesamt 53,3 Millionen Mark erpresst haben zu wollen.

Der Erpresser hatte versucht, „anonym" über das Internet seine Lösegeldforderungen und Drohbriefe zu übermitteln, die Details seiner Vorgehensweise wurden jedoch nicht veröffentlich. Bekannt ist, daß etliche Internet Service-Provider hier bei den Ermittlungen halfen, nachdem Teile des Kommunikationsweges nachvollzogen werden konnten. Dem Täter wurde vom Richter offenbar strafmildernd die Entwicklung eines Omnipotenzgefühls am Computer bestätigt.

Wußtet Ihr schon...?

...daß ein nicht unerheblicher Teil des BKA-internen Netzwerkes von der Fa. Debis betrieben wird?

...daß das Bundesamt für die Anerkennung ausländischer Flüchtlinge diese mit EDI verarbeitet?

...daß das Blacklisting bei GSM wirklich nur ein Blacklisting ist?

...daß man einen Geldautomaten offline bekommt, indem man in einer nahegelegenen Telefonzelle den Telefonhörer an einen Kuhzaungenerator anschließt? Die OvSt fährt dann offenbar wegen „Blitzeinschlag" runter.

...daß deswegen mitunter auch von „digitalen Cowboys" die Rede ist?!

Chaos Communication Congress 97

Auswahl von Berichten vom 14. Chaos Communication Congress, 27.-29.12.1997 Hamburg Eidelstedt

Die Texte stellen eine Auswahl aus der Congress-Dokumentation des 14. Chaos Communication Congress dar, der vom 27.-29. Dezember 1997 mit rund tausend Teilnehmern in Hamburg tagte. Die vollständige Dokumentation ist hoffentlich sehr bald schriftlich beim Chaos-Versand in Hamburg erhältlich. Die elektronisch vorliegenden Texte findet ihr unter http://presse.ccc.de

Sicherheit bei der Deutschen Telekom als Wettbewerbsfaktor

Referent: Jürgen Haag, Deutsche Telekom AG

Die Sensibilisierung des Personals für Sicherheitsbelange als eine Aufgabe des Zentrum für Netzsicherheit.

Die Gewährleistung der Sicherheit von Daten und Telekommunikation ist auf der einen Seite eine eindeutig technische Aufgabe. Da Sicherheit hohe Priorität genießt, ist die Kostenfrage bei technischen Lösungsansätzen meist zweitrangig.

Sicherheit ist aber auf der anderen Seite auch eine Frage des Verhaltens der Mitarbeiterinnen und Mitarbeiter. Nur wenn beide Faktoren zusammenwirken, ist der gewünschte Erfolg zu erzielen.

Unseren Kunden ist es letztlich gleichgültig, ob Sicherheitslücken aufgrund technischen oder menschlichen Versagens entstehen. Für sie ist nur das - in diesem Falle meist negative - Ergebnis von Interesse.

Viele technische Lösungen sind nur dann wirksam, wenn sie vom Mitarbeiter als feste Bestandteile des Arbeitsalltags akzeptiert und auch tatsächlich angewendet werden. Häufig findet sich jedoch die Einstellung, die technischen Sicherungsmaßnahmen reichten allein schon aus, um Eingriffe Unbefugter zu verhindern. Alltägliches Beispiel: Daten auf Einzelplatzrechnern können mit verschiedenen und fast immer vorhandenen Maßnahmen gesichert werden. Doch wessen PC ist tatsächlich verschlossen und mittels eine Paßwortes geschützt, das etwas komplizierter als der eigene Name, der Name (Kosename) der Frau oder des Mannes, oder das eigene Geburtsdatum ist? Oft wird auch der Inhalt der gespeicherten Daten im Hinblick auf das Erfordernis der Datensicherung unterschätzt. Schwer vorstellbar, welches Interesse Dritte zu Zeiten des Fernmeldemonopols an den Interna der Deutschen Telekom gehabt haben sollten.

Mit der Öffnung des Marktes und dem Eintritt in den Wettbewerb ist es jedoch mehr denn je erforderlich, maximale Sicherheit zu gewährleisten. Hierzu reicht eine Verbesserung der Technik allein nicht aus. Die Mitarbeiterinnen und Mitarbeiter, die mit dieser Technik arbeiten, müssen sich der besonderen Risiken und Anforderungen in diesem Bereich bewußt sein.

Die Sensibilisierung für Sicherheitsfragen und eine entsprechende Weiterbildung ist eine wichtige Maßnahme für die Beschäftigten zur Verhinderung des Mißbrauchs von Informationen und TK-Netzen und damit zur Abwendung eines hierdurch entstehenden wirtschaftlichen Schadens. Eine solche Sensibilisierung führt auch dazu, daß die bestehenden gesetzlichen Verpflichtungen, nämlich die Wahrung des Fernmeldegeheimnisses und des Datenschutzes, erfüllt werden.

Durch das Zentrum für Netzsicherheit wurde in enger Zusammenarbeit mit der Weiterbildung eine Seminarreihe entwickelt, die den Titel „Aktion Sicheres Netz“ trägt. Die Schulungen sollen bei den Beschäftigten ein Bewußtsein für das Thema Sicherheit nicht nur im Bezug auf die Netztechnik, sondern auch im Hinblick auf den verantwortungsvollen Umgang mit telekominternen Informationen am eigenen Arbeitsplatz schaffen.

In einer ersten Seminarreihe, die wir „Pilotmaßnahme Aktion sicheres Netz“ genannt haben, wurden Verhaltenstrainerinnen und -trainer der Bildungszentren in einem sog. „train the trainer“ geschult. Dabei wurde diesem Personenkreis vertiefte Kenntnisse vermittelt, u.a.

auch die Information, wie andere Firmen mit dem Thema „Sicherheit“ umgehen.

Diese Verhaltenstrainerinnen und -trainer geben ihr Wissen direkt an ca. 5000 Kräfte mit Führungsfunktionen des Unternehmensbereichs TN weiter. Die Schulungen dauern 2 Tage, an denen durch Gruppenarbeiten und Rollenspiele ein sicherheitsbewußtes Verhalten eingeübt wird. Aus didaktischer Sicht reicht ein Vortrag bzw. Frontalunterricht nicht aus, um tatsächlich eine Verhaltensänderung zu erzielen. Die eigenen fehlerhaften Verhaltensweisen müssen erkannt und sicherheitsbewußtes Verhalten eingeübt werden.

Diese ca. 5000 Führungskräfte erhalten den Auftrag, das erlernte Wissen in ihrem Verantwortungsbereich weiterzuvermitteln und umzusetzen. Für die Weitervermittlung werden die Führungskräfte mit Schulungsmaterial (Leitfaden, Video, Folien etc.) ausgestattet. Das Schulungsmaterial (Koffer) ist professionell erstellt worden und berücksichtigt didaktische und pädagogische Elemente.

Die geschulten Führungskräfte werden somit in die Lage versetzt, die selbsterfahrene Schulung an ihren Mitarbeitern und Mitarbeiterinnen weiterzugeben.

Vorstellung des Inhalts des Schulungskoffers:

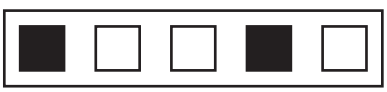
1. Seminarunterlagen Beinhalten a. ein didaktisches Konzept für den Dienstunterricht b. eine vertiefende Darstellung der 10 Sicherheitsregeln mit Beispielen aus der Praxis der einzelnen Zielgruppen c. Anleitungen für Einzel- und Gruppenarbeiten und Rollenspiele - Übung der Sicherheitsregeln. - Sicherheitsmängel in meinem eigenen Arbeitsumfeld. - Wie kann ich die Sicherheitsregeln an meinem Arbeitsplatz anwenden?
2. Plakate Diese dienen als Hinweis für die Schulungsveranstaltung
3. Video: a. Einführende Rede unseres VTN Gerd Tenzer. b. „Sind Meinungen Tatsachen?“, Darstellung der Deutschen Telekom im Deutschen Fernsehen. c. „Ein Tag wie jeder andere“. Spielfilm, der einen Tag bei der Deutschen Telekom beschreibt. Mit möglichen Sicherheitslücken und deren Bewältigung durch die Mitarbeiter/innen.
4. Folien
5. Diskette (Powerpoint)
6. Broschüre (zur Weitergabe an die Mitarbeiter/innen)

Ziel ist es, alle TN-Mitarbeiter und Mitarbeiterinnen - insgesamt ca. 70.000 Beschäftigte - in Sicherheitsfragen zu unterweisen. Der zu vermittelnde Inhalt besteht zunächst aus einem Überblick, was unter dem Begriff Sicherheit verstanden wird. Des weiteren soll verdeutlicht werden, wer von dem Wissen der Beschäftigten der Deutschen Telekom profitiert. Es soll aufgezeigt werden, welche Bedeutung Sicherheit als Wettbewerbsfaktor hat.

Kernstück dieser Aktion Sicheres Netz sind die folgenden Punkte, die griffigerweise in 10 Sicherheitsregeln gefaßt worden sind. Diese lauten:

1. Sie wissen mehr als Sie glauben
   - o Wissen kann mosaikartig zusammengesetzt werden.
   - o Unbedachte Äußerungen liefern wichtige betriebliche Informationen.
   - o Viele sagen, ich weiß ohnehin nichts.
   - o Mein Wissen ist doch allgemein bekannt.
   - o Negativhinweise geben Hinweise auf Schwachstellen. Auch die Informationen können für Wettbewerber nützlich sein.

2. Die Konkurrenz hat ein waches Auge
   - o Keine Interna an Wettbewerber.
   - o Besondere Achtsamkeit bei ehemaligen Kollegen, die jetzt z.B. beim Konkurrenten tätig sind.
   - o Bei Planungsverfahren nur die Informationen weitergeben, die wirklich benötigt werden.



- o Geplante Leistungsmerkmale mit Einführungsterminen und Zeitschienen.
- o Telefonverzeichnisse u.s.w. sind ebenfalls für die Konkurrenz sehr interessant.

3. Informationen sind unser Kapital
   - o Sämtliche Vertragsunterlagen geben tiefgreifende Einblicke.
   - o Sensible Informationen – ob auf Papier oder Diskette oder dem Laptop – nicht im Auto liegen lassen.
   - o Geplante Netzknotenstandorte sind für Wettbewerber sehr wichtig, denn sie verraten die Netzstrategiekonzepte der Deutschen Telekom. Mit diesen Informationen können Wettbewerber Einblicke in die Marktstrategie gewinnen und die eigene Planung darauf abstimmen.
   - o Datenträger jeder Art (Disketten, Bänder, MO-Disk, etc.) sind immer an sicheren und nicht frei zugänglichen Orten zu verwahren. o Keine Standleitungen unter Unix oder Windows offen stehen lassen; Datenpiraterie.

4. Erst sind die Daten weg, dann der Kunde
   - o Gebührendaten (Kommunikationsdatensätze) sind besonders sorgfältig zu behandeln.
   - o Es ist sicherzustellen, daß solche Daten nicht manipuliert werden
   - o Auch der Umgang mit statistischem Material über Verbindungsdaten,
   - o Verkehrsaufkommen und Anschlüsse muß mit großer Vorsicht erfolgen.

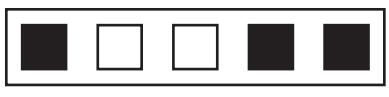
5. Wenn Sie ein Auge zudrücken, entgeht Ihnen manches
   - o Bei Kundenanträgen auf ungewöhnliche Umstände achten. 100 Anschlüsse in 30 m2 Raum.
   - o Auffälliges Verhalten von Kollegen, arbeitet am Rechner unter einer anderen als der eigenen Kennung, liest fremde Korrespondenz.
   - o Wahrgenommene Sicherheitsschwachstellen oder ungewöhnliche Vorkommnisse in der Umgebung nicht einfach ignorieren, sondern den Vorgesetzten darauf ansprechen.
   - o Kundenreklamationen ernstnehmen und auf mögliche Manipulationen hin auswerten.

6. Ein Paßwort ist keine stille Post
   - o Das Paßwort dient dazu, daß der Bediener sich im System eindeutig indentifiziert.
   - o Nicht aus Bequemlichkeit jemandem das eigene Paßwort mitteilen. Keine einfachen Paßwörter benutzen.
   - o Am besten ein Paßwort mit Buchstaben, Zahlen und Sonderzeichen. Möglichst nicht notieren.

7. Vorsicht beim Telefonieren - manchmal hören mehr Leute zu, als Sie denken
   - o Telefonische Auskunftsersuchen Fremder mit Skepsis begegnen. Offen herumstehende Anrufbeantworter sind ein Gefahrenpotential. Beim Weiterschalten eines Gespächs darauf achten, daß keiner mehr in der Leitung ist.
   - o Bei vertraulichen Telefonaten, die Türen schließen.

8. Ihr Papierkorb kann reden
   - o Beim Versenden von E-Mails, Vorsicht bei der Adreßeingabe.
   - o Wichtige Dokumente gehören nicht in den Papierkorb.
   - o Faxen über Kurzwahltaste. Vorsicht!
   - o Protokolle über den Ein- und Ausgang von rechtsverbindlichen Faxen führen.

9. Offene Türen und Fenster laden ungebetene Gäste ein
   - o Büros beim Verlassen verschließen.
   - o Verlust von Schlüsseln ist sofort dem Ressortleiter zu melden.



- Nach Dienstschluß Kontrolle durchführen, ob tatsächlich alle Räume und Fenster verschlossen sind.

10. Fragen Sie Fremde, wo sie hinwollen
    - Generell gilt der Grundsatz: Fremde sollen nicht ohne Begleitung durch das Haus gehen. Dies ist bei Kunden wie auch unbekannten Kollegen einzuhalten.
    - Fremde Personen, die sich alleine im Gang aufhalten fragen, wo sie hinwollen und dann begleiten.
    - Ganz besonders in Technikräumen sind Fremde unbedingt anzusprechen.

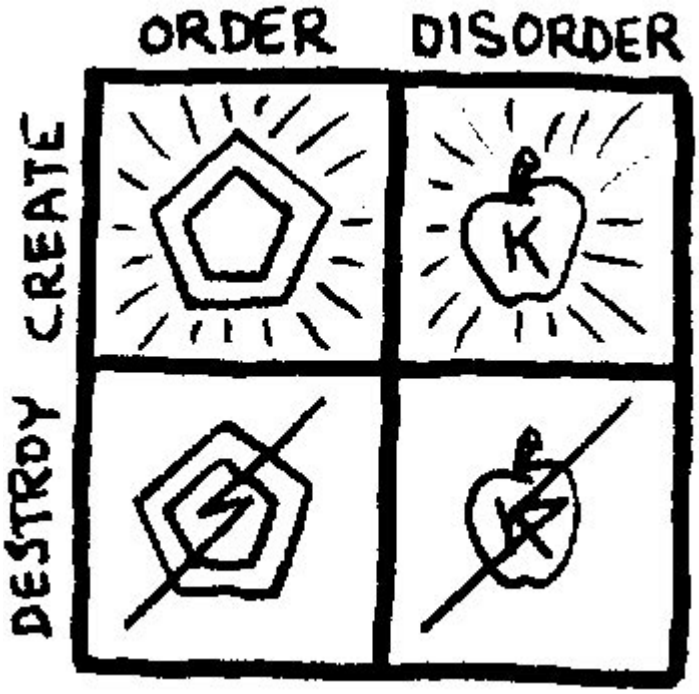
Diese 10 Sicherheitsregeln sollen in Rollenspielen eingeübt werden. Des weiteren soll der einzelne ausführen, wie er die Sicherheitsregeln an seinem Arbeitsplatz anwenden kann.

Hinweise auf Sicherheitsmängel oder auch Vorschläge können an das ZfN weitergegeben werden.

Evtl. mögen einzelne Regelungen für einzelne Bereiche überzogen wirken. Doch auch bei der Sensibilisierung der Mitarbeiter gilt, daß mit gesundem Menschenverstand gearbeitet werden muß. Nicht alle Verhaltensweisen sind für alle Bereiche gleich verbindlich. Das eigene Know-how sollte jedoch auf keinem Fall unterschätzt werden.

Die oben aufgeführten Regeln tragen dazu bei, daß das Sicherheitsbewußtsein der Beschäftigten steigt und damit das Vertrauen der Kunden in die Deutsche Telekom erhalten bleibt. „Sicherheits-pannen“ bzw. „-lücken“ müssen möglichst vermieden werden. Der wirtschaftliche Schaden durch sie ist immens. Nur wenn der Kunde Vertrauen in die Sicherheit seiner Daten und der Telekommunikation hat, werden neue Dienste der Deutschen Telekom auch angenommen. Doch wie bereits oben ausgeführt: Sicherheit kann es nur geben, wenn die Technik sichere Lösungen bietet und die Mitarbeiter und Mitarbeiterinnen, die mit dieser Technik arbeiten, sich dieser besonderen Risiken und Anforderungen bewußt sind und entsprechend verhalten.

Die „Aktion Sicheres Netz“ ist eine erste Maßnahme, der noch weitere folgen sollen, um kontinuierlich einen hohen Stand an Sicherheitsbewußtsein zu halten. Mit einer hohen Sicherheit erzielt die Deutsche Telekom einen entscheidenden Erfolgsfaktor im künftigen Wettbewerb.



Einführung in Theorie und Praxis: Verschlüsselungsalgorithmen und Implementationen

Referenten: Andreas Bogk, Lutz Donnerhacke

Versteckt vermittelte geheime Nachrichten sind so alt wie die Menschheit. Sklaven wurden Mitteilungen auf den gescherten Kopf tätowiert und sie gingen mit dichtem Haarwuchs auf die Reise. Der Empfänger scherte die Haare wieder ab und brauchte danach nur noch den

Sklaven zu köpfen, um höchste Geheimhaltung zu gewährleisten.

Cäsar soll im römischen Reich den „Cäsar Cypher“ erfunden haben, bekannt als ROT 13, wonach alle Buchstaben eines Textes um 13 Stellen weiter im Alphabet verschoben werden (fb jvr va qvrfrz Orvfcvry). Diese Verfahren verändern nur das Erscheinungsbild eines Textes, Eigenschaften bleiben dagegen erhalten. So ist der Buchstabe ‘e’ das häufigste Zeichen in deutschsprachigen Texten - der Ausgangspunkt zum Buchstabenraten.

Mit den Kriegen stiegen auch die Ansprüche: Neue Verfahren wurden entwickelt und alte Verfahren wurden komplexer. Die „Enigma“ (Verschlüsselungsmaschine der deutschen Wehrmacht im zweiten Weltkrieg) arbeit mit sieben sich gegeneinander verschiebende Scheiben die ihre Position nach jedem Zeichen ändern. Ein finnischer Mathematiker erkannte, daß trotz dieses Aufwandes nur das Erscheinungsbild des Originaltextes verändert wurde. Mit erheblichem Aufwand konnten die Nachrichten nun mitgelesen werden.

Auguste Kerckhoffs beschreibt die Voraussetzungen für eine sichere Verschlüsselung folgendermaßen: „Ein Verfahren ist dann sicher, wenn man es nicht knacken kann, obwohl man den Code kennt.“

Struktur des modernen Verschlüsselungsalgorithmus

Die Nachricht wird mit einem Schlüssel verschlüsselt. Der entstandene verschlüsselte Text wird nun sicher verschickt und vom Empfänger entschlüsselt. Der Schlüssel muß natürlich auf einem sicheren Weg übermittelt werden.

Wenn der Empfänger einen anderen Schlüssel als der Absender benutzt, kann der Schlüsselaustausch entfallen. Moderne Verschlüsselungsalgorithmen sind z.B. IDEA oder DES. Die Anwendung und Kombination von Algorithmen ergeben dann die Verschlüsselungsprotokolle, mit denen man im Alltag zu tun hat. Moderne Verschlüsselungsprotokolle sind z.B. PGP oder S-MIME.

Was passiert beim Verschlüsseln?

Unterschieden wird zwischen Stream-Verschlüsselung und Block-Verschlüsselung.
Stream-Verschlüsselung (Stream-Cypher)

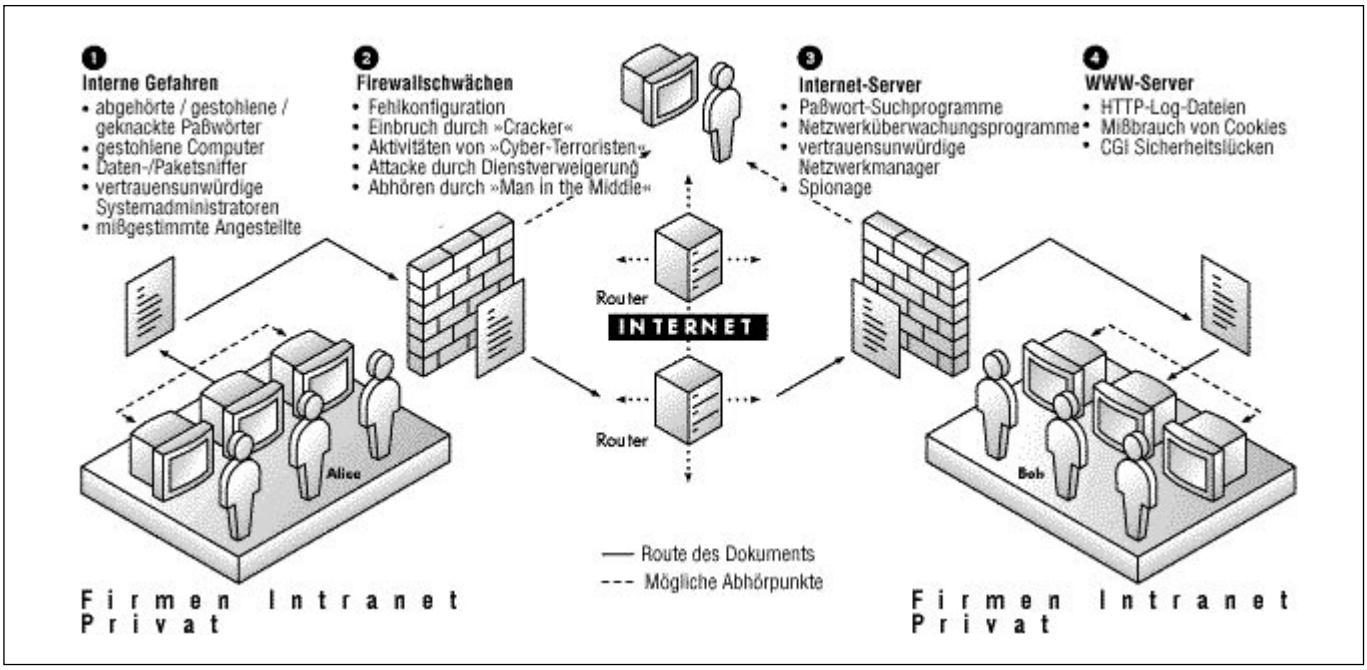
Bei der Stream-Verschlüsselung wird die Nachricht byteweise, manchmal sogar bitweise verschlüsselt. Die Encryption-Engine liefert Zahlenfolgen die mit den Datenstrom per XOR verrechnet werden. die Encryption-Engine benutzt dazu z.B. den Key und einen (Pseudo-) Zufallszahlengenerator. Ein Pseudo-Zufallszahlengenerator (linearer kongruenter Generator) erzeugt Zahlenfolgen für den Hausgebrauch. Die Wahrscheinlichkeit der Zahlenfolgen ist voraussagbar. Ein „echter“ Zufallszahlengenerator benutzt eine natürliche Zufallsquelle (z.B. Zählung des radioaktiven Zerfalls eines Elements).

Block-Verschlüsselung

Arbeitet mit definierten Blöcken (z.B. 1 Block = 256 Byte). Das bietet den Vorteil effektiver nachvollziehbare Wiederholungen durch die Verschlüsselung zu vermeiden. Nach der ersten Verschlüsselung finden dann noch weitere Verschlüsselungen statt. Rückkopplungen und Verknüpfung mit anderen Blöcken erzeugen komplexere verschlüsselte Texte (z.B. mit Block-Shiften).

Angriffsvarianten auf verschlüsselte Daten

Nachdem man den bevorzugten Ort der eigenen Wahl gefunden hat, um die Daten zu bekommen, steht die Wahl der erfolgreichsten Attacke.



Cyphertext ist vorhanden

Die schwierigste Ausgangssituation für eine Entschlüsselung sind nur die verschlüsselten Daten vorhanden. Über deren Inhalt ist nichts bekannt. Die ganze Vielfalt der Entschlüsselungspalette, von geschicktem Raten bis zur Häufigkeitsanalyse, kann nun darauf angewendet werden, ohne daß eine Verfahren schneller zum Erfolg führt als ein anderes.

Known-Plaintext-Attack

Von den verschlüsselten Daten sind Teile bekannt, wie z.B. feste Grußformeln in Briefen oder Dateiheader in Computerdaten. Verschlüsselten Fisch erkennt man z.B. schnell am Geruch.

Chosen-Plaintext-Attack

Hier unterscheidet man zwischen den Überprüfungsmöglichkeiten seiner Ergebnisse:

1. Eine einzige Überprüfungsmöglichkeit - beim Benutzen der Erkenntnisse aus den entschlüsselten Daten sitzt am anderen Ende z.B. der andere Geheimdienst und ein Fehler fällt sofort auf.
2. adaptive-chosen-plaintext - Dem Computer am anderen Ende ist es egal, wie oft ich meine falschen Entschlüsselungen an ihm austeste.

Gummiknüppel-Attacke

Bei der Gummiknüppel-Attacke geht man davon aus, daß mich die verschlüsselten Daten erwarten. So befinden sich auf einer Festplatte mehrere Dateisysteme die sich gegenseitig nicht kennen. Entschlüssele ich nun ein Dateisystem und greife darauf zu, erkennt es den Rest der Festplatte als ungenutzt an und belegt sie. Die anderen Dateisysteme werden dadurch gelöscht.

Brute-Force-Attacke

Der simpelste Angriff - ich probiere alle Möglichkeiten durch. Im Zeitalter der krebsartig wachsenden Computerkapazitäten ist brute-force inzwischen eine zeitsparende Variante. In Kombination mit anderen Attacken läßt sich der Weg zu den Originaldaten schnell eingrenzen.

Text: Mo Hataj

Chaos Communication Congress 97

Auswahl von Berichten vom 14. Chaos Communication Congress, 27.-29.12.1997 Hamburg Eidelstedt

Open Source Processing – Geheimdienst zum Selbermachen

Referent: Frank Rieger

Der Begriff „Open Source Processing“ läßt sich am einfachsten mit „Verarbeitung von Daten, die öffentlich zugänglich sind“ beschreiben. Dabei entstehen erst durch eine sinnvolle Filterung und Aufbereitung Informationen. Werden Informationen so weit aufbereitet, daß sie entscheidungsrelevant werden, kann man von Botschaften oder englisch von Intelligence sprechen. Geht man von den einzelnen Daten aus, so läßt sich durch 7 W-Fragen (Wer?, Was?, Wann?, Wo?, Mit wem?, Warum? und Womit?) ein Ereignis ziemlich exakt beschreiben (der Referent, in der ehemaligen DDR aufgewachsen, sprach von den „7 Stasi-Fragen“). Dabei können die verschiedensten Formen von „Open Sources“ genutzt werden, z.B. Bibliotheken, deklassifizierte Daten, Zeitschriften und Zeitungen, kommerzielle Informationsdienste und Datenbanken, CD-ROMs und das Internet.

Diese Informationsquellen werden nicht nur von Privatleuten genutzt; so ziehen z.B. die Geheimdienste ca. 80% Ihrer Informationen aus offenen Quellen. Diese werden dann weiterbearbeitet, und erst durch den Gewinn an Informationsinhalt gehören sie dann zu den Geheimdaten. Man geht davon aus, daß der größte Teil der Geheiminformationen der Geheimdienste aus Zeitungsausschnittsammlungen besteht. „Altbundeskanzler Schmidt hielt die ‘Neue Zürcher Zeitung’ für aktueller und akurater als BND-Lageinformationen“, wie Frank Rieger meinte.

Durch den rapiden Preisverfall bei Computerleistung und Speichermedien ist es jetzt auch jedem Privatmenschen möglich, eine große Menge an Daten zusammenzuführen und nach persönlich relevanten Kriterien zu verarbeiten, dabei faßt eine 4 GB-Platte eine Volltext-Datenbank von 1 Million Seiten.

Eine mögliche Anwendung hierzu wurde am Rechner demonstriert, indem die Daten der CD-ROM „D-Info“ mit denen der CD „Gewußt wo!“, einem Branchenverzeichnis für bestimmte Großräume, in diesem Fall die Stadt Berlin, zusammengeführt wurden und so zu jeder Berliner Adresse eine geographische Koordinate ermittelt wurde. Aus den 1,3 Millionen Telefonteilnehmern Berlins konnte so ein „telefonischer Stadtplan“ erstellt werden, in dem die verschiedensten Suchen möglich sind:

- Telefonvermittlungsstellenbezirke
- die Bevölkerungsdichte, bzw. bei bekannter Bevölkerungdichte schlechter situierte Randgebiete
- Stadtviertel mit einem hohen Ausländeranteil (Suche nach ausländischen Vornamen/Namen)
- wenig besiedelte Gebiete mit einem hohen Anteil an Frauen als Telefonanschlußinhaberinnen
- Standorte für Existenzgründungen
- Suchen nach nicht-gelisteten Telefonnummern, dabei ist eine Eingrenzung auf wenige Straßen ist meist möglich, in

ländlichen Gebieten manchmal sogar eine Eingrenzung auf das einzelne Haus...

Eine Verknüpfung mit weiteren Datenquellen (Newsgroups, Homepages mit Foto, T-Online-Kennung) ermöglicht zu identifizierten Personen dann eine Erstellung eines Personenprofils. Wenn man verschieden alte Daten miteinander vergleicht, kann man mit verschiedenen Ausgaben der „D-Info“ z.B. schon Aussagen über Migrationen und Veränderungen der sozialen Struktur erhalten.

Für die persönliche Nutzung kann man sich zum Beispiel im Internet umschauen, wo man eher das Problem hat, daß die Informationsmenge zu groß ist und sie nur mit großem Aufwand auf ein sinnvolles Maß reduziert werden kann. Man kann problemlos personenbezogene Informationen, Produkt- oder Firmen-Informationen beschaffen. Einige Internet-Dienste bieten auch Informationsprocessing an, so liefert z.B. Paperboy automatisch generierte Pressespiegel des Tages und deckt dabei 90% der deutschen Zeitungen ab.

Sucht man Informationen über Personen und deren Interessensgebiete, so hilft eine Abfrage bei Deja News. Wenn man auf komerzielle Datenbanken oder Informationsdienste zugreift, so hat man meist eine geradezu kryptische Benutzeroberfläche und zahlt gelegentlich gutes Geld für Informationen, die anderswo kostenlos erhältlich sind. Außerdem geht man hier das Risiko ein, daß die Abfragen in Abfrageprofilen ausgewertet werden.

Bei allen Informationen, die man sich beschafft, hat man aber immer gewisse Probleme, und zwar zunächst die Bewertung der Glaubwürdigkeit:

- Ist die Quelle bekannt?
- Gab es aus dieser Quelle schon Fehlinformationen?
- Besteht die Gefahr einer gezielten Desinformation?
- Wie sind die Eigentums- und Einflußverhältnisse bei der Quelle?
- Wie aktuell sind die Daten (gerade CD-ROMs sind oft schon veraltet, wenn sie auf dem Markt sind)?
- Hat man parallele Quellen zur Überprüfung?
- Sind die Daten vollständig?

Bei der Archivierung der Daten kommen dann die nächsten Probleme: Die Datenmengen und Informationsvielfalt macht kooperatives Arbeiten mehrerer Personen notwendig. Eine sinnviolle Indexierung ist schwierig; die Informationsqualität läßt sich nicht aus der Anzahl der verwendeten Quellen ableiten. Der Fluß der Aufbereitung (Data -> Information -> Intelligence) muß beherrscht werden.

Insgesamt wurde gezeigt, daß sich heutzutage sehr genaue Informationssammlungen auch von Privatleuten mit vertretbar geringem Aufwand erzeugen lassen. Deshalb muß man auch mit seinen eigenen Daten entsprechend bewußt umgehen, da Firmen die verfügbaren Informationsquellen in jedem Fall auswerten - ganz zu schweigen von den Geheimdiensten.

Text: Derk Marko Reckel

Chaos Communication Congress 97

Auswahl von Berichten vom 14. Chaos Communication Congress, 27.-29.12.1997 Hamburg Eidelstedt

ISDN für Anfänger – Protokolle und Netzfunktionen

Referent: Hartmut Schröder

Zunächst zur analogen Telefonie: In der analogen Telefonie werden Sprache oder Daten durch sinusförmig modulierte Frequenz-änderun-gen in der Leitungsspannung übertragen. Dabei entstehen einige Probleme, z.B.:

- die Parallelschaltung der Endgeräte erzeugt ein Echo, das man hört, bzw. das ein Datensender auch wieder empfängt
- bei einer Übertragung über eine gewisse Distanz ist eine ein- oder mehrmalige Verstärkung des Signals nötig, wodurch eine Verschlechterung der Qualität eintritt

In der digitalen Telefonie wird der Spannungswert der Modulation in Zeittakten abgetastet (8000 Hz), es wird ein Zahlenwert erzeugt, der an die Gegenstelle übermittelt wird. Die Gegenstelle stellt dann die Spannungshöhen aus den Zahlenwerten wieder her und glättet sie zu einer Kurve.

Durch die digitale Übertragung als 0 und 1 kann auf die Verwendung von Verstärkern auf weite Distanzen verzichtet werden, weil die Signalunterscheidung auch bei sehr langen Leitungen möglich ist.

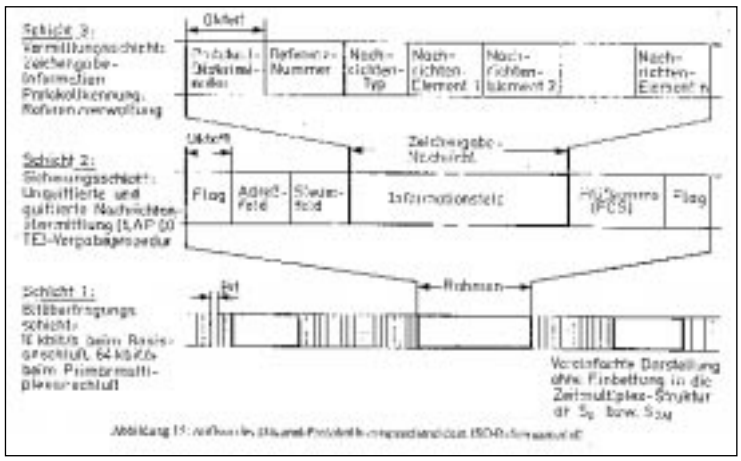
Die theoretischen Grundlagen für diese Technik wurden 1940 gelegt. Durch neuere Übertragungstechniken konnten zunächst 2 und dann ca. 10 Gespräche über ein und dieselbe Leitung übertragen werden.

Bei den ISDN-Anschlüssen muß man zwischen zwei Anschlußarten unterscheiden:

- Primärmultiplex-Anschluß (Europa: 30 B-Kanäle (64 kBit), 1 D-Kanal (64 kBit), 1 Synchronisierungskanal (64 kBit) USA/Japan: 23 B-Kanäle (Japan 64 kBit, USA 56 kBit), 1 D-Kanal(Japan 64kBit, USA 56 kBit), 1 Synchron-Kanal (16 kBit)
- und dem für Endverbraucher gedachten Basisanschluß: Euro/USA/Japan: 2 B-Kanäle (64 kBit, USA 56 kBit), 1 D-Kanal (64kBit, USA 56 kBit), 1 S-Kanal (16kBit)

(B-Kanal: Gesprächskanal, Kommunikation der Teilnehmer D-Kanal: Kommunikation der Geräte)

Die Abfolge der Daten im D-Kanal wird dabei in einem 7-Schichtenmodell codiert, wobei die



definierten Schichten 4, 5 und 6 meist nicht verwendet werden.

ISDN Schichtenaufbau Referenzmodell der ISO
7. Schicht: Anwendung
(6. Schicht: Darstellung)
(5. Schicht: Sitzung)
(4. Schicht: Transport)
3. Schicht: Vermittlung, Zeichengabeinformation, Protokollkennung, Referenzverwaltung
2. Schicht: Sicherungsschicht und quittierte Nachrichtenübermittlung
1. Schicht: Bitübertragungsschicht (physikalische Signalübertragung)

Für die 3. Schicht gibt es je nach Land unterschiedliche Protokoll-Normen, auch beim Euro-ISDN gibt es länderspezifische Unterschiede im Leistungsumfang (Rückruf bei besetzt, Rufnummernübermittlung und Gebühren-übermittlung sind nicht in allen Ländern verfügbar).

Für die Übertragung wird zunächst das Sprachsignal als 12 Bit repräsentiert, und anschließend auf 8 Bit geschrumpft. Bei der Umsetzung haben die USA eine andere Kennlinie (μ-Law) als der Rest der Welt (A-Law). Beim Konvertieren zwischen den Ländern entstehen Verluste, die sich bei Sprache nicht auswirken. Für eine Datenübertragung muß deshalb signalisiert werden, daß es sich um einen Datenanruf handelt, sonst entsteht durch die Konvertierung reiner Datenwust.

Physikalisch kommt beim Teilnehmer mit einem ISDN-Basisanschluß eine 2-adrige Leitung an den „Übergabepunkt", den NT (in Deutschland NTBA), der NT ist eine Bus-Installation (Punkt zu Mehrpunkt-Installation) mit interner und externer Terminierung, die 4-adrig zu den Endgeräten geht. Auch bei der ISDN-Übertragung bekommt man auf das Signal ein Echo, daß durch Laufzeitbestimmung herausgerechnet wird (Echo-Kompensator).

Gesendet wird mit 144 kBit, das zu 120 kBit verwürfelt wird (ternäre Übertragung: es werden nicht nur 1 und 0 gesendet, sondern auch -1, damit kommt es nicht zum Ladungsaufbau (Kapazitäten), die Flanken der Signale bleiben vielmehr steil.

Wie passiert die Kommunikation?

Das Anmelden der Endgeräte bei der Verbindungsstelle und das Protokoll zum Verbindungsaufbau zwischen zwei Teilnehmern findet sich in dieser Beispieldatei im Detail vorgestellt. Dies geht weit über den Umfang einer Anfänger-Veranstaltung hinaus. Für Interessierte findet sich das verwendete Programm unter: http://www.mms.de/~hacko/d-tracy).

Datenübertragung

Zur Datenübertragung werden weltweit 4 Protokolle verwendet:

- V.110: spezifiziert bis 19200, keine Fehlerkorrektur, inzwischen obsolet („V.JEHOVA")
- V.120: terminalgebundene Datenübertragung mit voller Ausnutzung der Bandbreite („ist O.K.")
- X.75: nur ein kleiner Bereich des Protokolls wird verwendet. Man definiert Fensteranzahl und Blockgröße, meist verwendet: BLK 2048 W(indow)S(ize) 7; („wird bald verschwinden")
- P.SYNC-PPP(RFC1717): verwendet zwischen ISDN-Routern, für Internet Zugänge (der heutige Standard).

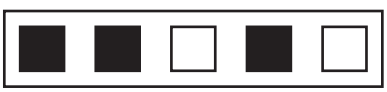
Text: Derk Marko Reckel

Packet Radio - Eine Einführung

Datenfunk im Amateur- und CB-Funkdienst
Referent: Henning Heedfeld [DG1YGH]

Packet-Radio ist ein paketorientierter Datenfunk im Amateur- oder CB-Funkdienst. Zur Zeit werden als gängige Übertragungsgeschwindigkeiten 1.200 und 9.600 bit/s eingesetzt. Als Netzwerk-Standard wird das AX.25-Protokoll verwendet, ein speziell für den Amateur-Datenfunk modifiziertes X.25-Protokoll. Bei Übertragungsgeschwindigkiten bis 2.400 bit/s kann man mit handelsüblichen Funkgeräten arbeiten, der Anschluß funktioniert direkt über die Mikrofon-Buchse des Funkgerätes. Bei höhereren Übertragungsgeschwindigkeiten muß aufgrund der höheren Bandbreite eine Modifikation im Funkgerät vorgenommen werden: das Sendesignal wird dann hinter dem FM-Diskriminator eingespeist.

Als Modem können zwei Gerätearten eingesetzt werden: die preiswertere Lösung bietet 1.200 bit/s und besteht aus einem Operationsverstärker sowie einigen passiven Bauteilen. Dieses sogenannte PCCOM-Moden kostet im Selbstbau rund 20 DM oder ist für ca 100 DM



fertig aufgebaut im Fachhandel zu beziehen. Es ist ein passives Gerät, die Protokollumsetzung und Auswertung erfolgt über eine zusätzliche PC-Software.

Als zweite Möglichkeit, die grundsätzlich vorzuziehen ist, können sogenannte TNCs (Terminal Node Controller) eingesetzt werden. TNCs sind sowohl für 1.200 bit/s als auch für 9.600 bit/s erhältlich oder preiswert im Eigenbau zu realisieren. Im Eigenbau entstehen Kosten von rund 150 DM, ein Fertiggerät kostet zwischen 250 und 350 DM. Ein TNC hat eine eigene, meist Z80-basierende Microcontroller-Steuerung und kann somit auch autark betrieben werden.

Die Ansteurung durch den PC erfolgt über einen eigenen Befehlssatz. TNCs bieten ausserdem die Möglichkeit, im sogenannten Transparent-Modus betrieben zu werden. Somit kann mittels PPP oder SLIP eine TCP/IP-Verbindung aufgebaut werden. Im Praxistest wurden in einer Punkt-zu-Punkt-Funkstrecke über 7 km rund 300 Byte/s Datendurchsatz erreicht (70cm Band, 9.600 bit/s übertragungs - geschwindigkeit im Simplex-Betrieb). Wesentlich höhere Übertragungsraten können nur durch Modifikation auf 19200 bit/s oder unter Einsatz einer Vollduplex-Verbindung erreicht werden, da dann die Hochtastzeiten der Funkanlagen wegfallen.

Nachteilig ist hierbei, daß auf beiden Seiten doppeltes Equipment benötigt wird.

Unklar ist bei einer solchen TCP/IP-Verbindung, über die ja auch Internet geroutet werden kann, die rechtliche Lage. Funkgeräte für 9.600 bit/s sind zur Zeit nur im Amateurfunkdienst legal zu betreiben bzw. zu modifizieren. Der Amateurfunkdienst darf nur von lizensierten Funkamateuren betrieben werden. Das Amateurfunkgesetz verbietet allerdings die Verbindung von Funkanlagen mit anderen Kommunikationsnetzen. Außerdem ist die Übermittlung von verschlüsselten Daten nicht zulässig.

Die legale Alternative wäre der CB-Funk (Citizens Band = Jedermannsfunk). Da der CB-Funk im Kurzwellenbereich betrieben wird, ist ein effektiver Funkbetrieb aufgrund von Störungen in der Regel nicht möglich. Desweiteren müssen im CB-Funk zugelassene Funkgeräte verwendet werden. Somit stehen nur Geschwindigkeiten von 1.200 bit/s zur Verfügung. Unter anderen rechtlichen Umständen wäre so eine preiswerte Realisierung von Wireless-LANs möglich, die auch mit wesentlich höheren Geschwindigkeiten betrieben werden können.

Von der Kommunikations- zur Informationsgesellschaft: Dummheit in Netzen

Teil 14: „Keine Bewegung“
Referent: padeluun

Alle Jahre wieder wacht padeluun in einem Workshopraum auf und spricht über dumme Sachen. Und wie jedes Jahr sitzen da Leute, die der festen Meinung sind, sie machen gar keine dummen Sachen. Am Ende haben alle recht.

Zusammenfassend gesagt: Die Retrospektive über die Alpträume der Electrosphäre war harmloser als in den letzten Jahren; Ideen und Mittel für konstruktive Technikentwicklung sind gefunden, es muß aber weniger gejammert und mehr umgesetzt werden.

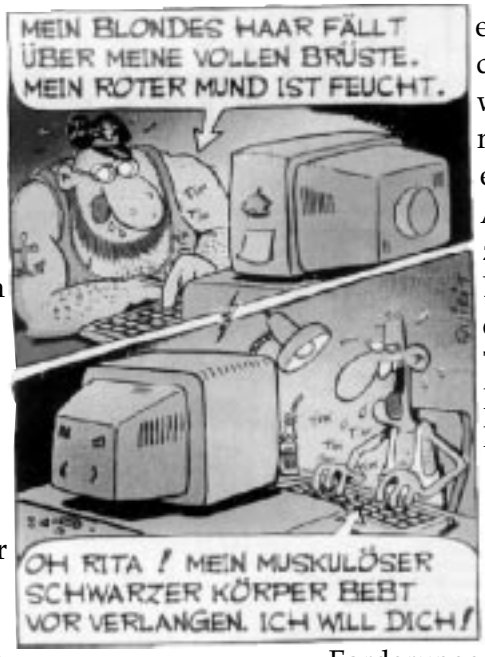
Nach dem Internet-Hype schämt sich padeluun, sich als Mailboxbetreiber zu outen. Als „Systembetreiber“ spart er sich Häme und Daseinsberechtigungsdeklaration im Sysadmin-Environment. Die Standleitung ersetzt im Denken das Kommunikationsnetzwerk, die lebendige Online-Community taucht im Denken der IP-Persönlichkeiten selten auf.

Auf einem Telekom-Servicewagen prangt inzwischen „Kommunikation verbindet - Freundschaft vereint“. Diese Grundhaltung ist inzwischen bei PR-Agentur und Vorstand verbrei-

tet, CCC-Thesen der letzten Jahre tauchen immer öfter in der „realen“ Welt auf.

Was davon zu halten ist, sei dahingestellt. Als Chaos-Computer-Club, -Communication-Congress und -Szene ist der Schritt vom Meckern zum Ändern nicht getan worden. Trotz Pesthörnchen gegen den Gilb und Teufel gegen Telekom mußten erst Service-Training-Center und business reengineering für besseren Service von Telekom-Hotlines sorgen.

Wäre schön gewesen, wenn das vor 10 Jahren bereits passiert wäre. Klar, die Leidensfähigkeit der betroffenen Bevölkerung war damals höher und jede/r Aufrechte ein Terrorist. Die Probleme waren aber richtig im Kern erkannt, Phantasie und Aktionen sammelten sich ums Meckern.



Klammheimlich migrierten Chaos-Ideen und -Forderungen in den Alltag. Diverse RFCs, die Erfindung der Telefon-Hotline, die Erfindung der Mailbox haben gerade auf dem Congress tiefe Wurzeln. Diese Lichter stehen heute noch unterm Scheffel und kommen dort wohl auch nie mehr raus. So geht es auch vielen Menschen aus der Szene hier, sie leben nicht das Leben, das sie sich wünschen, und haben Haltungen eingenommen, die ihren Interessen widerstreben. Abseits von „Fremdsteuerung“ und „Illuminaten-Paranoia“ existiert das Problem, seine Visionen endlich einmal zu verwirklichen. Geld kann dabei sicherlich nicht das Ziel sein, sondern eher: Arbeiten um zu leben.

Chaos-Leute jonglieren heute zwischen Spiegel-Anfragen und Netnite-Interviews. Vom anfänglichen Interesse der Produktions-gesellschaften, man hätte ja viel gemeinsam als „Hacker“ mit weltaufklärerischer Intention, bleibt bei der Abrechnung der schale Nachgeschmack, nur als Figur aus der Szene vorgeführt worden zu sein.

„Wellen kann man reiten, nicht lenken“ (Bismarck) und enden sie immer am Strand?

Das Internet ist ein tolles Recherchemedium mit vielen ruhenden Informationen. Erst Aktivität schafft Bewegung. Neben „Bayrischer Hackerpost“ und „Datenschleuder“ existierte Peter Glasers „Labor“, damals verpönt durch geringere Technikzentrierung und zeitaufwendiges Layout. „Konr@d“ kann als direkter Nachfolger gesehen werden, Kritik hin oder her, die Selbstbekenntnis, ein buntes Heft zu machen, ist in der Nullnummer abgedruckt, wenn die Chaos-Themen hier massenkompatibel werden, kann es nur besser werden.

Auf dem Kongreß kennt jeder zehnte mindestens fünf Bundestagsabgeordnete - hier ist eine riesige Machtkonzentration. Trotz allem existiert ein Phänomen im Netz: Die Hemmung der User, sich um ihre eigenen Bedürfnisse zu kümmern. Dabei geht es nicht mal um Eigenaktivität, als Jürgen Tauss (MdB SPD) um eine Zusammenfassung der Forderungen aus einer Newsgroup bat, passierte wochenlang nichts - außer das weiter über die Forderungen diskutiert wurde. Das zweistündige Thesensammeln für eine Anhörung zum TKG im Bundestag wurden nicht realisiert.

So ist der Wandel der „Kommunikations-gesellschaft“ zur „Informationsgesellschaft“ ein Bild dieser Quasselnetze, jede/r redet mit, keine/r mehr miteinander.

Text: Mo Hataj

Medien

CD-Rom: „Hacker“ von Hemming

Im September erschien die CD „Hacker“ von Hemming. „Nur wer die Werkzeuge der Hacker kennt, kann sich wirksam schützen“ steht drauf. Sie wird für rund 25 DM vertrieben und enthält eine interessante Sammlung von Shareware. Alle Programme lassen sich in mehreren Sprachen installieren und wieder deinstallieren. Außer Virenschutz gibt es drei Crackprogramme. KOS hat ein hübsch langes Dictionary, dann FZC, ein brute force Angriff auf PKZIP und PGP-Crack v0.6b.

Disassemblieren und dekompilieren läßt sich einiges außer VB, auch Java-Klassen. Außer Hex-Editoren, Patchprogrammen und Schutzprogrammen ist auch PGP 2.6.3.i mehrsprachig (de/it/cz/fr/es/nl) drauf; leider ohne die regelmässig in de.org.ccc geposteten PGP-FAQ´s. Die Schutzprogramme auf der CD sollen einen gewissen Mindestschutz vor den mitgelieferten Zerlegeprogrammen bieten. In der Regel wird das Ei aber klüger als die Henne. Zielgruppe der CD ist nicht der kleine Hacker von nenebenan, sondern eher Entwickler.

Unter „Diverses“ wird auch der CHAOS COMPUTER CLUB erwähnt. Einige Texte zum activeX-Hack sind drauf, aber auch Adressen und Ansprechpartner des CCC. Gesamturteil: nicht negativ. Nur der Klappentext „Unerlaubtes Kopieren und Verleihen untersagt“ ist im Zeitalter, wo Silberlinge teurer sind als Goldlinge, lächerlich.

„HACKER“

`http://www.hemming.de`

wau@ccc.de

Termine

CeBIT ‘98

Das Weltcentrum der Büro- und Informationstechnik steht immer noch in Hannover. Dieses Jahr ist der Chaos Computer Club auch wieder mit dabei.

CCCeBIT98
HANNOVER
19.—25.03.1998

Ihr findet uns in Halle 22/Stand A16. Tägliche Workshops ergänzen unseren Auftritt um einen „kleinen Congress“.

23

Der Kinofilm über den Hacker Karl Koch kommt nach derzeitigen Erkenntnissen am 12. November 1998 (12 + 11 = 23!) in die deutschen Kinos.

Public Domain #84

A2 privat – Morgenwelt im Abendland

“Wenn der Staat kein Geld hat, um seinen Aufgaben nachzukommen, ist es Zeit ihn abzuschaffen und die Geschäfte einer Privatfirma zu übergeben. Wenn ein Land sich finanziell nicht mehr lohnt, wird es eben stillgelegt.“ – Hartwig Thomas erzählt über Privatisierung und die Folgen.

Sonntag, 5. April 1998 ab 15 Uhr Bunker Ulmenwall Bielefeld

`http://www.foebud.org`

REINHARD RUPPRECHT
MINISTERIALDIREKTOR
IM BUNDESMINISTERIUM DES INNERN

[redacted] Bonn
Fernruf: (02 28) [redacted]
oder [redacted] (Vermittlung)
Telefax: (02 28) [redacted]

den 19. Dezember 1997

Herrn
Andy Müller-Maguhn
MdV Chaos Computer Club e. V.

per Fax

Sehr geehrter Herr Müller-Maguhn,

herzlichen Dank für Ihre freundliche Einladung zur Teilnahme an einer Diskussionsrunde im Rahmen des CCC, die Sie ja schon bei unserem Zusammentreffen in München am 18. November andeuteten.
Den bisher vorliegenden Informationen nach haben Sie ein weit gespanntes Spektrum an Themen und Aktivitäten geplant. Meine Person und meine Grundauffassungen würden da aber wohl als störender Fremdkörper empfunden. Eine Konfrontation „alle gegen einen" will ich aber den Kongreßteilnehmern nicht zumuten. Diese sind sicher weniger - so nehme ich an - an „Wirtschaftsspionage und Innerer Sicherheit" und umso mehr an der breiten Palette technischer Probleme interessiert.

Ich wünsche Ihnen und der Veranstaltung gutes Gelingen und Ihnen persönlich alles Gute zum Neuen Jahr.

Mit freundlichen Grüßen

Bestellungen, Mitgliedsanträge und Adreßänderungen bitte senden an:

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

Adreßänderungen auch per Mail an office@ccc.de

Der Mitgliedsfetzen

Mitgliedsanträge und Datenschleuderabonnement

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

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

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

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

Die Kohle liegt

o als Verrechnungsscheck
o in Briefmarken

bei bzw.

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

Ort/Datum

_____

Unterschrift

_____

Name

_____

Straße

_____

PLZ, Ort

_____

Tel/Fax

_____

Der Bestellfetzen

Literatur

_____ DM 42,00 Mailbox auf den Punkt gebracht
_____ DM 29,80 Deutsches PGP-Handbuch, 3. Auflage + CD-ROM
_____ DM 5,00 Doku zum Tod des „KGB“-Hackers Karl Koch
_____ DM 25,00 Congressdokumentation CCC ‘93
_____ DM 25,00 Congressdokumentation CCC ‘95
_____ DM 50,00 Lockpicking: Über das Öffnen von Schlössern

Alte Datenschleudern

_____ DM 50,00 Alle Datenschleudern der Jahre 1984-1989
_____ DM 15,00 Alle Datenschleudern des Jahres 1990
_____ DM 15,00 Alle Datenschleudern des Jahres 1991
_____ DM 15,00 Alle Datenschleudern des Jahres 1992
_____ DM 15,00 Alle Datenschleudern des Jahres 1993
_____ DM 15,00 Alle Datenschleudern des Jahres 1994
_____ DM 15,00 Alle Datenschleudern des Jahres 1995
_____ DM 15,00 Alle Datenschleudern des Jahres 1996

Sonstiges

_____ DM 50,00 Blaue Töne / POCSAG-Decoder / PC-DES Verschlüsselung
_____ DM 5,00 1 Bogen „Chaos im Äther“
_____ DM 5,00 5 Aufkleber „Kabelsalat ist gesund“

+ DM 05,00 Portopauschale!

_____ Gesamtbetrag

Die Kohle liegt

o als Verrechnungsscheck (bevorzugt)
o in Briefmarken

bei bzw.

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

Name

_____