Jörg Osarek Unternehmensberatung
Triftstr. 30, D-61350 Bad Homburg
Germany
Mobil: +49 (0)151 / 23 0 24 333
Email: jo@beraterexzellenz.de
USt-IdNr.: DE 231 411 298
Steuernr. 003 854 31634

Computerviren - historischer Artikel von 1989

von Jörg Osarek

eine Neuauflage zum zwanzigjährigen Jubiläum des Artikels

Vorwort aus dem Jahr 2009

Diesen Artikel habe ich im Jahr 1989 geschrieben. Dank aufgehobener Disketten meines Atari ST konnte ich nun eine Konvertierung des Textes und der Bilder vornehmen und den Artikel "restaurieren" - die Bilder wurden damals auf meinem Atari ST u.a. mit einem 3D-CAD Programm erstellt und dann weiter von mir kombiniert.

Was zum Thema Computerviren damals in Ansätzen erkennbar war, ist heute die Realität einer großen Industrie für digitale Sicherheit, welche gegen Viren, Würmer, Trojaner, Phishing und vieles mehr kämpft. Vor dem Hintergrund dieser Entwicklung stellt sich die spannende Frage: Wie wird die Welt der Computerviren in weiteren zwanzig Jahren aussehen - also im Jahr 2029?

Ich bin überzeugt wir werden interessante und bedrohliche sowie gleichzeitig faszinierende und erschreckende Ereignisse sehen. Computerviren mutieren weiter zu künstlichen Lebensformen und die Virenindustrie wird sich zu einer Art elektronischem Gesundheitswesen weiterentwickeln. Wir werden gegen diese Schädlinge Nützlinge einsetzen und eine digitale Biosphäre - ein zweites Ökosystem - entstehen sehen, eine "Gaia 2.0" sozusagen (siehe Gaia-Hypothese).

Doch nun zurück zu dem Artikel, den ich vor zwanzig Jahren geschrieben habe, einerseits aus Neugierde, um das Thema selbst besser einordnen zu können und andererseits, um für die Leser eine gewisse Klarheit zu schaffen. Es sollte sich von selbst verstehen, dass die Tipps, die ich seinerzeit gegeben habe, heute nicht mehr sinnvoll anwendbar sind - vor allem: Schalten Sie nicht einfach Ihren Rechner aus, Sie könnten die Software-Installation beschädigen. Heutzutage besorgen Sie sich am Besten einen guten Virenscanner und bewegen sich mit einer gewissen Umsicht im Internet. Doch der letzte Tipp von vor zwanzig Jahren ist auch heute noch wertvoll: "Immer auf dem Laufenden bleiben".

Ihr Jörg Osarek, 19. November 2009

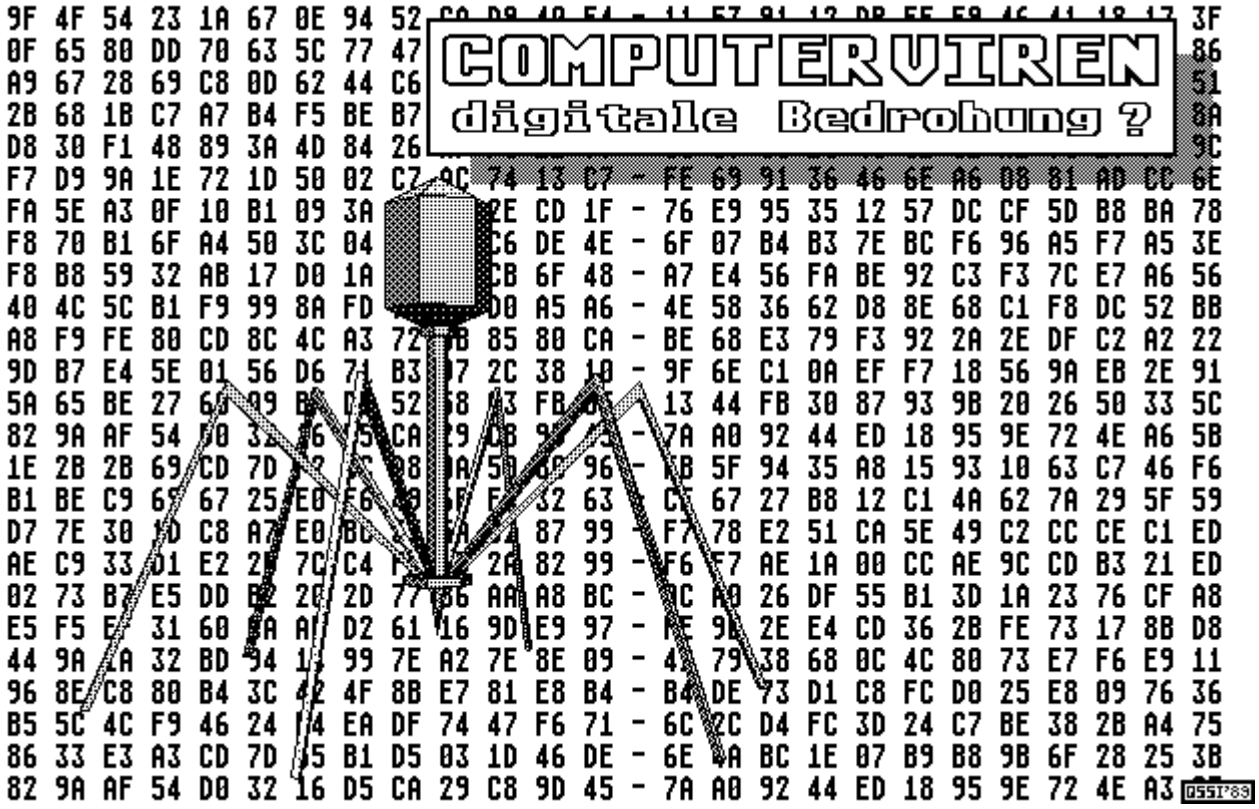
Ergänzung im Juli 2010

Das Internet ist schon eine Goldgrube. In einer Diskussion auf xing.com wurde ich auf frühere Anfänge hingewiesen. Das gab mir die Gelegenheit, diese Angaben zu ergänzen. Besten Dank für die Anmerkungen.

Bereits 1953 entwickelte John von Neumann die Theorie selbstreproduzierender Automaten. 1975 verbreitet sich der Virus Pervade auf UNIVACs und 1982 infiziert der Elk Cloner Viren Apple II Computer.

Eine weiterführende Übersicht findet sich in einem Artikel von cnet von Robert Lemos aus dem Jahr 2003.

COMPUTERVIREN - DIGITALE BEDROHUNG ODER PANIKMACHE?



In der letzten Zeit ist viel über Computerviren geredet, geschrieben und berichtet worden. Man hört von trojanischen Pferden, Würmern, logischen Bomben und elektronischen Seuchen. Die Informationsflut ist groß, und da noch durchzublicken ist garnicht so einfach.

Fangen wir also ganz von vorne an.

Die ersten Ansätze und Theorien wurden wohl Mitte bis Ende der siebziger Jahre entwickelt. Fred Cohen schrieb mit die ersten Viren und veröffentlichte eine ausführliche Dokumentation dazu, die nicht nur auf Begeisterung stieß. 1981 stellte er folgende Definition auf:

> *"We define a computer virus as a program that can infect other programs by modifying them to include a possibly envolved copy of itself. With the infection property, a virus can spread througout a computer system or network, using it to infect their programs."*

Zu Deutsch:

> *"Wir definieren einen Computervirus als ein Programm, das andere Programme infiziert, indem es sie dahingehend modifiziert, eine eventuell veränderte Kopie seiner selbst in diese einzuschließen. Durch die Infektions-Eigenschaft verbreitet sich ein Virus innerhalb eines Computersystems oder Netzwerks, indem es dieses benutzt, um die Programme seiner Anwender zu infizieren.*

Ein Virus ist also erst einmal ein Programm. Nichts weiter. Es kann in jeder beliebigen Programmiersprache geschrieben werden, wie z.B. Modula 2, C, Fortran, Cobol, Pascal oder auch in Basic. Es gibt sogar einen "LOGO"-Virus.(Logo ist eine recht einfach zu erlernende Programmiersprache.) Damit ein Programm als Virus bezeichnet werden kann, muß es die zwei folgenden Eigenschaften haben:

- Es muß sich vermehren können und
- Es muß eine bestimmte Funktion ausführen können.

In der Regel besitzt ein Virus auch noch einen Auslöser für die Funktion. Der Funktionsteil wird also nur aufgerufen, wenn der Auslöser "zündet". Z.B., wenn ein bestimmtes Datum erreicht ist (Freitag der 13.), oder wenn der Vorname des Benutzers "HELGA" ist, oder wenn der Virus die fünfzigste Kopie von sich selbst erstellt. Der Auslöser wird eingebaut, damit der Virus nicht so schnell entdeckt wird. Dadurch hat er Zeit sich ungestört zu verbreiten, bevor er dann oft lawinenartig gezündet wird.

Damit wissen wir nun, wie ein Virusprogramm aussehen kann. Es verfügt über eine Vermehrungsroutine, eine Funktionsroutine und meist über eine Auslöserroutine. Aus dem Hauptprogramm werden diese Routinen aufgerufen, oder sie sind darin integriert.

Jetzt, wo klar ist, was ein Virus ist, kann man diese auch abgrenzen von den berühmten "Nichtviren". Am häufigsten werden wohl trojanische Pferde zu Viren gezählt, obwohl sie genausoviel mit Viren zu tun haben, wie ein Dachziegel mit einem Butterbrot.

Ein böser User, nennen wir ihn mal Ossi, schreibt dieses Programm und kopiert es in den öffentlichen Account (Public) unter dem Namen "EDIT". Sein Kollege Kasi ruft eines schönen Morgens seinen Editor mit dem Namen "EDIT" auf. Der Computer ruft nun jedoch erst den "EDIT" aus dem Public Account auf, da er diesen zuerst findet. Das trojanische Pferd gibt in unserem Beispiel nun alle geschützten Dateien von Kasi frei, d.h. jeder kann diese Dateien nun aufrufen. Danach ruft unser Pferd den normalen Editor auf, und was unser guter Kasi davon mitbekommen hat ist Nullkommanichts. Genauso wird es jedem anderen User gehen, der das Programm "EDIT" aufruft. In relativ kurzer Zeit wird der böse Ossi nun auf sehr viele Dateien zugreifen können, die er eigentlich garnicht benutzen dürfte. Irgendwann löscht er sein trojanisches Pferd im Public Account und keiner hat etwas gemerkt.

Die beschriebene Methode kann z.B. beim Betriebssystem UNIX angewendet werden.

Ein anderer "Nichtvirus" ist die "logische Bombe". Es ist vielmehr ein gezielt plaziertes Programm, das sich nicht vermehrt und irgendwann vom Programmierer an der Stelle gezündet wird, an der es plaziert wurde. Auch die Tannenbäume, die weltweit durch sämtliche Mail-Systeme verschickt wurden und die Rechner überlasteten, bis sie zusammenbrachen, waren keine Viren, sondern Kettenbriefe, die von den Usern weitergegeben wurden. Selbst der häufig zitierte "Virus" in der Raubkopie des Programms "Larry Lover", der bei erreichen einer Score von 222 Punkten ohne Vorwarnung die Festplatte formatiert, ist keiner. Die Herstellerfirma selbst hat diese Vorrichtung eingebaut, damit das Programm nicht raubkopiert wird.

Die meisten Viren infizieren Programme. Es gibt aber auch Bootviren, die sich im Bootsektor der Diskette befinden. Der Bootsektor ist ein Sektor aufder Diskette, der beim Start des Rechners automatisch durchgearbeitet wird.Ist ein solcher Virus im Bootsektor wird er beim Start aktiviert und kopiert sich beim nächsten Diskettenwechsel in den Bootsektor der neueingelegten Diskette. Nach gleichem Prinzip arbeiten Batchviren, die in Batchdateien abgelegt werden, die ebenfalls beim Rechnerstart abgearbeitet werden. Sie kommen jedoch äußerst selten vor.

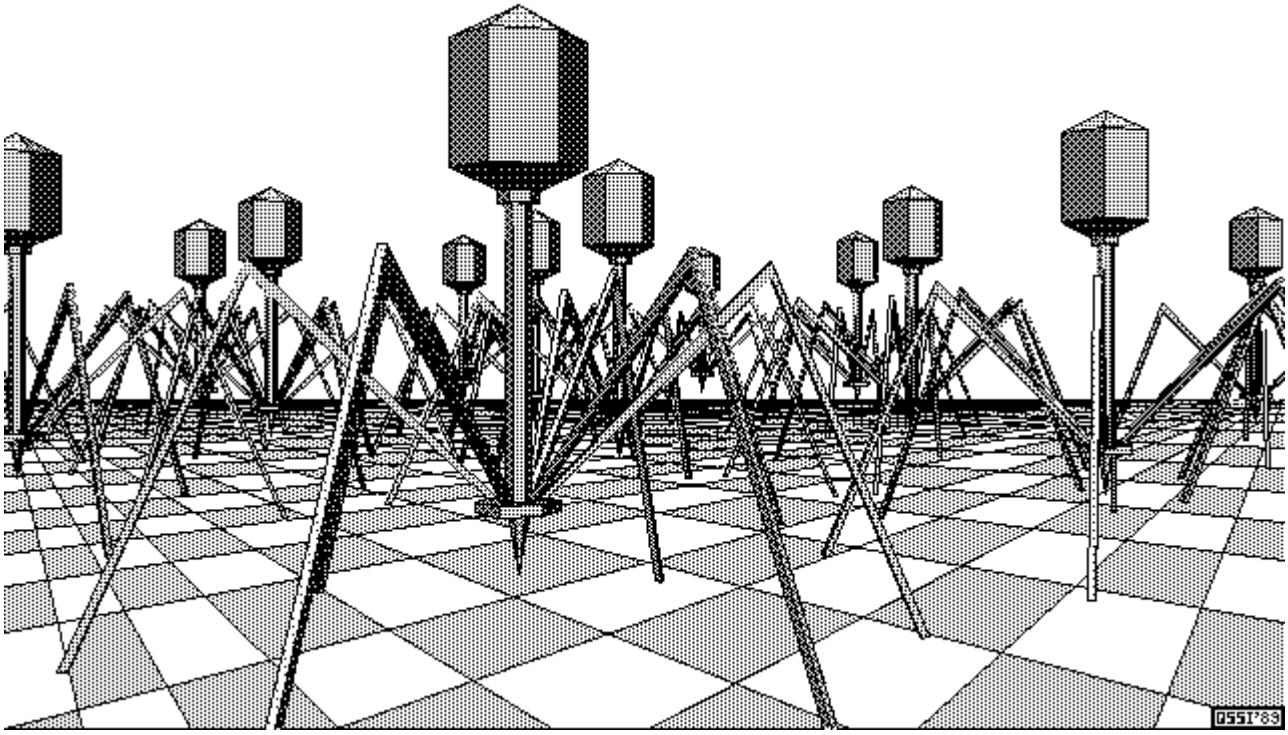
Größtenteils werden ausführbare Programme von Viren befallen. Wie geht so etwas nun vor sich? Die einfachste Methode ist, der Virus pflanzt sich vor das Programm. Beim nächsten Aufruf des infizierten Programms wird zunächst der Virus abgearbeitet, sucht sich ein noch nicht infiziertes ausführbares Programm und verseucht es auf die gleiche Weise. Andere Viren setzen sich hinter oder sogar in das Programm hinein, oder sie setzen nur einen Sprungbefehl in das Programm, der den irgendwo anders auf einem externen Speicher abgelegten Virus aufruft. All diese Viren verändern die Länge des Programms. Durch den Längenvergleich mit einem garantiert virenfreien Backup (Kopie) des Programms kann man also eine Modifikation leicht entdecken. Raffinierter Viren komprimieren einen Teil des Textsegments des Wirtsprogrammes, bevor sie sich einpflanzen um genau die Länge, die der Virus einnimmt. So verändert sich auch die Programmlänge bei der Infizierung nicht mehr.

Zur Zeit bringen die meisten Viren wohl die Besitzer von größeren Homecomputern wie etwa Schneider, Atari-ST und Commodore Amiga zur Verzweiflung, gefolgt von Viren die auf MS-DOS Rechnern ihr Unwesen treiben. Einige Fälle machten jedoch auch "Geschichte":

- Spätsommer 1988 New York: Ein Virus unbekannter Herkunft hat die Computerdatenbanken mehrerer US-Regierungsstellen zerstört. Betroffen ist auch eine Datenbank der NASA. Rund hundert Rechner wurden von dem Virus befallen. Er zerstörte Akten und verzögerte Projekte. Hunderte von Stunden wurden damit verbracht, den Virus unter Kontrolle zu bekommen.
- Robert Tappan Morris, Sohn eines führenden Computerwissenschaftlers in den USA setzte am 2. November 1988 einen harmlosen Computervirus im Internet aus. (Internet ist ein Zusammenschluß von über 12.000 Rechnern von Universitäten, großen Herstellerfirmen und militärischen sowie zivilen Forschungseinrichtungen) Morris nutzte kleine Fehler in Betriebssystemen und Mailsystemen für die Verbreitung seines Virus aus. Durch einen winzigen Programmierfehler im Virus wurden die Rechner mit den Viruskopien "bombardiert" und brachen zusammen. [Anmerkung aus 2009: Es handelt sich nach heutiger Auffassung um einen Computerwurm, nicht um ein Virus - den sogenannten Morris-Wurm]
- Am 13.1.1989 trat in England ein PC-Virus in Kraft, der auf einen "Freitag den 13." wartete. Er löschte Daten und Programme. Schlimmste Betroffene: ein britisches Unternehmen mit ca. 400 verseuchten PCs.
- In Israel kursierte ein Virus, der am 40. Jahrestag des Landes aktiv wurde und Datenbestände zerstörte. Er war vorher bekannt. Deswegen schalteten viele Leute ihre Computer an diesem Tag nicht ein, oder verstellten das Datum.
- Bei den Softwarehäusern Omikron und GfA-Systemtechnik wurden versehentlich mehrere tausend Programmdisketten mit harmlosen Bootsektorviren verkauft. Ein Viruskillerprogramm wurde so schnell wie möglich an die Käufer geschickt.

Wer nun einen Virus schreiben will, muß ein gewisses "Know-how" über Programmierung und seinen Computer mitbringen (wenn auch nicht allzuviel; wiegesagt: man kann auch in BASIC Viren schreiben.). Rainer Becker von der GFE (Gesellschaft für Finanz- und EDV-Beratung) in Bad Soden ist der Initiator des Virus Construction Sets. Mit dem VCS können mit bester Menüsteuerung Bootsektor- und Linkviren (Viren, die Programme infizieren) mit verschiedensten, auch selbst geschriebenen, Funktionen problemlos und bequem erzeugt werden. Das VCS ist auf dem Atari-ST erschienen, laut einem Artikel der Zeitschrift "mc", soll jedoch auch eine MS-DOS Version des VCS erscheinen. Mit einem solchem Programm ist es jedem, der weiß, wie man einen Computer einschaltet und eine Maus bedient, möglich, zerstörerische Viren freizusetzen. Glücklicherweise bedient sich der Virus immer der gleichen Vermehrungsroutine. (eigentlich ist es der gleiche Virus, Auslöser und Funktion sind variabel.) Deshalb kann man ihn leicht erkennen.

Bis jetzt ging es immer nur darum, daß Viren Software modifizieren oder zerstören. Doch auch die Hardware ist teilweise gefährdet. So gibt es einen MS-DOS Virus, der bei PCs mit Hercules Grafikkarte eine Nachricht in die Phosphorbeschichtung des Monitors brennt. Ein anderer Virus läßt die Diskettenstation ein Lied spielen, indem der Schreib-/Lesekopf von Anschlag zu Anschlag gefahren wird. (Das bekommt dem Gerät auch nicht allzu gut.) Auf ähnliche Weise zerstört ein Virus das Diskettenlaufwerk in kürzester Zeit. Auch Headcrashs bei Festplatten können von Viren verursacht werden. (Bei einem Headcrash schlägt der Schreib-/Lesekopf (S/L-Kamm) gegen die Festplatte und reißt Stücke heraus.) Besondere ICs, die wenig genutzt werden, erhitzen sich beim Einsatz recht schnell und gut. Wenn ein Virus diesen Chip ständig auf Trab hält, ist er schnell überhitzt und zerstört. Auch die Ports (Schnittstellen) bzw. die ICs, die diese verwalten sind Angriffsziel von Viren.



Wie kann man sich nun vor Viren schützen?

Ich habe vorhin schon einmal den Längenvergleich von Programmen angesprochen. Aber es existieren ja Viren, die die Länge der Programme nicht verändern. Um Schreib-/lesefehler auf magnetischen Datenträgern zu vermeiden werden von Programmen/-blöcken Prüfsummen errechnet und verglichen (VCR, CRC etc.).

Wenn ein Virus ein Programm auch längenmäßig nicht verändert, wird die Prüfsumme sich von der des Originalprogramms unterscheiden. So läßt sich der Virus dann trotzdem orten. Nicht jeder Computerbenutzer, gerade wenn es sich um einen reinen Anwender handelt, ist in der Lage ein Programm zu schreiben, das z.B. eine CRC-Prüfung durchführt.

Inzwischen vertreiben einige Firmen Vergleichsprogramme oder sogar Virenkiller, die die Viren erst auf oben beschriebene Weise entdecken und teilweise auch entfernen können. So bietet G DATA ein "Anti-Viren-Kit" an. Sterling Software macht Werbung für "comparex", eine Vergleichssoftware nicht nur für Viren.

Man kann sogar Disketten bzw. Platten gegen bestimmte Viren impfen. Wenn solche Programme existieren, warum gibt es dann noch immer Probleme mit Computerviren? Die Virenprogrammierer entwickeln eben immer neue Tricks, um den Viruskillern zu entgehen. Deswegen ist auch noch kein Ende abzusehen. Auf den Schutz Nr. 53 folgt ein Virus mit Trick Nr. 54, der dann doch durchkommt. Folge: Viren und Abwehrprogramme werden immer komplizierter. Ein Wettlauf, vielleicht ohne Ende und ohne Gewinner. Denn ein Allheilmittel gegen Viren gibt es nicht und wird es auch nicht geben.

Also wiegesagt: Der beste Schutz ist dieses Vorbeugen mit solchen Programmen. Leider habe ich im Büro noch keine solche Software unter die Augen bekommen, denn erstens ist es den Leuten wohl zu aufwendig (klar, wer will schon seine teure Zeit für so etwas verplempern) und zweitens ist wohl noch nicht genug passiert, als daß die Mitarbeiter sagen würden, so etwas sei jetzt schon nötig. Es ist nun einmal Tatsache, daß man erst aus Schaden klug wird. Erst wenn die Bombe eingeschlagen hat, wird man überlegen, was man dagegen tun kann.

Doch auch ansonsten kann man Vorsicht walten lassen:

- keine "Public Domain" Software im Büro verwenden. (PD-Software ist freie Software, die kostenlos weitergegeben werden darf. Wer will kann den Programmierern freiwillig eine kleine Entschädigung überweisen.) PD-Software ist eine gute Einrichtung, doch leider auch ein riesiger "Ansteckungsherd" für Viren.
- keine Raubkopien im Büro verwenden. Für Raubkopien gilt das gleiche wie für PD-Software. Für Zuhause: Solche Software und PD-Soft auf jeden Fall überprüfen !!!
- Backups (Sicherheitskopien) von Originalsoftware anfertigen und die Backupdisk nur zur Überprüfung benutzen.
- Disketten sauber trennen zwischen garantiert virenfreien und unsicheren Disks (Disketten, bei denen man nicht 100% sicher ist, daß sie virenfrei sind.).
- regelmäßige Backups der Arbeitsdisketten. Der Verlust an eigenen Daten ist oft weit schlimmer, als der Verlust von Programmen. Da stecken nämlich oft Stunden und Tage harter Arbeit drin.
- In regelmäßigen Abständen Programmvergleiche durchführen wie oben beschrieben. Auch wenns schwerfällt.

Wenns dann mal gekracht hat...

wenn man plötzlich ernsthafte Anzeichen eines möglicherweise in Aktion getretenen Virus feststellt (Formatiergeräusche, Wirrwarr auf dem Bildschirm etc.):

- SOFORT DEN RECHNER AUSSCHALTEN !!! Lieber einmal mehr ausschalten, als nachher die böse Überraschung einer völlig leergefegten Festplatte oder ähnliches zu erleben.
- In der Firma am besten gleich die EDV-Abteilung anrufen.
- Datenrettung. Sicherung der noch vorhandenen Arbeitsdateien. Mit schreibgeschützter Originaldiskette das Betriebssystem laden (Nicht von der Festplatte booten !!!), die Festplatte formatieren und alle Applikationen neu installieren. (Also wenns erst einmal passiert ist, macht das eine ganze Menge Arbeit. Auch deshalb: Vorbeugen.)

Als letzten Tip hätte ich noch anzubieten:

- IMMER AUF DEM LAUFENDEN BLEIBEN

7. Juni 1989 Jörg Osarek

Für die Hilfe bei der Erstellung dieses Berichtes möchte ich mich noch einmal bedanken
bei Jennifer Dähn, Helmut Debes, Carsten Kaiser, Ralf Lenz, Arnold Willemer.