Wissenschaftliche Projektarbeit über die Veranstaltung
„Aktuelle Probleme der IT- und Netz-Sicherheit“
für die Baccalaureatsprüfung

Auswirkungen des aVTC auf die Bedrohung der computerisierten Welt durch Malware und der Wintertest 2000/2001

Angefertigt bei Herrn Prof. Dr. Klaus Brunnstein
Fachbereich Informatik
Universität Hamburg

Vorgelegt von Kay Fiolka
30.03.2001

Inhaltsangabe

Abkürzungsverzeichnis

AV	Antiviren
aVTC	Antiviren-Testcentrum Hamburg
CARO	Computer Antivirus Research Organisation
EDV	Elektronische Datenverarbeitung
FAT	File Allocation Table, Dateizuordnungstabelle
ICQ	I seek you, Internet-Angebot zum bspw. Chatten
IRC	Internet Relay Chat
IT	Informationstechnologie
ITW	In The Wild, im Umlauf
Malware	malicious ware (bösartige Software)
mIRC	wohl bekanntester Klient für IRC
MS	Microsoft
NT	New Technology
NTFS	New Technology File System
PDA	Personal Digital Assistant, Handcomputer
PR	Public Relation
VBA	Visual Basic for Applications
VBS	Visual Basic Script
W2K	Microsoft Windows 2000
WAP	Wireless Application Protocol

Abbildungsverzeichnis

1. Einleitung

Die folgende Baccalaureatarbeit behandelt das Thema der Bedrohung der computerisierten Welt durch Malware und die Auswirkungen von Institutionen wie dem aVTC auf eben diese.

In Zeiten, in der die Bedrohung durch fast tägliche neue Schreckensmeldungen über neue Viren, Würmer, Trojaner oder sonstige für den Laien häufig einfach als Virus synonym gesetzte Malware, allgegenwärtig gemacht wird, wächst neben der Bedeutung kommerzieller Anbieter von Antiviren-Software auch die Notwendigkeit der Existenz von gesellschaftlichen Institutionen, die ohne Gewinninteresse, Informationen über diese Gefahr und deren Bekämpfer sammeln und auswerten. Für diese Institutionen, die das Thema Bedrohung durch Malware nicht fatalistisch sehen, sondern versuchen einen Beitrag zur Minimierung und Bekämpfung zu leisten, muß es auch in ihrem Sinne sein, daß sie objektiv und wissenschaftlich nach Sinn und Unsinn, Nutzen und Kosten evaluiert werden. Nur so kann eine Effizienzsteigerung und gegebenenfalls eine Umschichtung der Schwerpunkte zwecks besserer Zielrealisierung erreicht werden. Genau diese Überprüfung ist einer der Hauptaugenmerke dieser Arbeit.

Für die Überprüfung der Auswirkungen auf Anwender und AV-Industrie wurde ein individueller Fragenkatalog zusammengestellt, der viele Sachverhalte, die in späteren Kapiteln ausführlichst benannt werden, verdeutlichen konnte. Für die freundliche Unterstützung und rege Beteiligung bei der Beantwortung dieser Fragen möchte sich der Autor dieser Arbeit noch einmal sehr herzlich bedanken.

Des weiteren wird in dieser Arbeit auf den Wintertest 2000/2001 des aVTC und seine Ergebnisse, auch im Vergleich zu älteren Tests, im Detail eingegangen. Neben dem objektiven Testergebnis per se werden auch noch die subjektiv gemachten Erfahrungen als Projektleiter bei der Planung und der Durchführung beschrieben.

Abgeschlossen wird diese Arbeit durch eine Zusammenfassung und einen Ausblick auf das, was aus Sicht des Autors in nächster Zeit von diesem Thema zu erwarten ist.

Soweit in der nachfolgenden Arbeit Markennamen zitiert wurden, sind im Zuge des intellektuellen Eigentumvorbehalts sämtliche Rechte inkl. dem Copyright zu beachten.

2. Die Bedrohung

Die Bedrohung durch Malware gewinnt zunehmend an Bedeutung. Vorbei sind die Zeiten, wo sich die Verbreitung solcher Malware im Schwerpunkt auf das rege gegenseitige Austauschen von Daten auf Disketten beschränken mußte.

Heute stehen durch die zunehmende Vernetzung der Gesellschaft mit PCs statt Terminals und der wachsenden Ausdehnung des Internets und dessen Dienste wie insbesondere der E-Mail ganz andere Möglichkeiten zur Verfügung, die die Ausbreitung eines Virus wie in einem Zeitraffer exponentiell anwachsen lassen kann.

Virus : W97M.Melissa
Typ : Makro-Virus, VBA
Erstes Auftreten : 26.03.1999 in alt.sex
Infektion : Word-Dokumente und -Vorlagen
Verbreitung : sehr hoch, verbreitet sich über e-Mail
Trigger : wenn Minute der Stunde = Tag, Bsp: am 14. eines Monats zu jeder Stunde XX.14
Plattform : Word97, Word2000, Outlook 97 oder 98
zstzl. Schadroutine : verschickt sich und das zum Zeitpunkt des Triggers befallene Dokument an die Kontakte aus dem Adreßbuch, entfernt Funktion „Makros deaktivieren“ in der Registry

Allein in Deutschland gehen die jährlichen Kosten durch Virenbefall in Unternehmen nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mittlerweile in die Milliarden. Genaue Zahlen dafür gibt es aber nicht, da viktimologische Untersuchungen gezeigt haben, daß viele Unternehmen aus Angst vor Negativwerbung zögern, ihre Einbußen und Schäden durch Cyber-Angriffe offen darzulegen. Gerade in sicherheitssensiblen Branchen wie Banken und Versicherungen oder in Bereichen die sich auf dem EDV-Sektor spezialisiert haben, wie Soft- und Hardwarefirmen, ist die Angst vor einem Imageverlust sehr groß. Wenn man aber optimistisch rechnet, daß für jeden der ca. 10 Mill. in Deutschland geschäftlich genutzten PCs DM 100,00 für Schulung und Software anfallen, ist man alleine bei der Minimalvorsorge schon in den Milliarden.

Aus Sicht des BSI-Virenexperten Frank Felzmann ist die weltweite Dominanz von Microsoft-Programmen eine der Gründe für das Übel [1]. Diese Ansicht vertreten laut einer Umfrage der Internet World vom 09.05.2000 [2] auch fast 3/4 der

befragten Personen, wobei sich diese Zahl incl. der 17% versteht, die das nicht auf Microsoft reduzieren, sondern insgesamt die Monokultur verantwortlich machen, egal welches Betriebssystem diese Monokultur darstellt. Da ca. 90% aller Computer unter Windows-Betriebssystemen laufen, sei der Viruseffekt ein ähnlicher, „wie wenn der Borkenkäfer in monostrukturierte Waldplantagen“ (Frank Felzmann) einfiele.

Durch das undifferenzierte Einräumen von Rechten zum Überschreiben, Verändern und Löschen von Programmen ist das Windows-Betriebssystem der ideale Nährboden für bösartige Software.

Einer der eindrucksvollsten Angriffe der letzten Zeit war sicherlich der als Liebesbrief getarnte „Loveletter“-Virus, der Anfang Mai 2000 das erste Mal gemeldet wurde. Im Zuge des schneeballartigen Verbreitens des Virus über die Adreßbücher der MS Outlook-Nutzer wurden, so nach Schätzungen verschiedener Computerexperten, zwischen 70 und 90 Prozent aller Unternehmen weltweit von dem Virus befallen. In Anzahl befallener Rechner ausgedrückt, geht man von 50 Millionen aus, was ein Anteil von ~20 % des damaligen Gesamtbestandes der Rechner weltweit ausmachte. Bei Schadensabschätzungen verschiedener Medienblätter (bspw. Bild, Focus, Spiegel) rangierten die Zahlen zwischen 5 und 50 Mrd. weltweit. Will man aber einen Schaden abschätzen, muß man sich erst einmal auf eine gemeinsame Definition von Schaden einigen. Der objektive Teil der Definition beschreibt wertfrei den tatsächlichen Ablauf, den Vorgang, den Teil „was ist passiert ?“. Bei der Beantwortung dieser Frage werden im Zuge des „Loveletters“ sicherlich unter anderem

Virus : I-Worm.LoveLetter
Typ : Wurm, VBScript-Wurm
Erstes Auftreten : 04.05.2000
Besonderheiten: kann sich auch über mIRC verbreiten, installiert zusätzlich einen Trojaner
Verbreitung : extrem hoch, nutzt die Mappi-Schnittstelle, um sich über Outlook an alle Adressen des Adreßbuches zu verschicken
Plattform : MS Outlook 98/2000, Windows Scripting Host muß installiert sein
zstzl. Schadroutine : der installierte Trojaner liest unter anderem Paßwörter des Rechners und sendet sie an den Host, macht Dateien verschiedenster Extension unbrauchbar

folgende Fakten genannt werden: Verlust von Daten, Arbeitsstundenausfall durch Säuberung der Rechner, Zurückspielen von Sicherheitskopien etc. Nun gibt es aber noch den subjektiven Teil der Definition, der sich mit dem eigenen Anteil beschäftigt, mit der Frage des vorsätzlichen, fahrlässigen und unvermeidbaren Handelns. Wie hoch muß man den subjektiv aufgetretenen Schaden berechnen, wenn man bedenkt, daß der „Loveletter“ mit einfachsten Sicherheitsvorkehrungen und -maßnahmen, vorher hätte abgefangen werden können? Firmen müssen endlich die Notwendigkeit von Sicherheitsschulungen und –management erkennen, endlich hinreichend in künftige Sicherheit investieren, endlich verantwortlich mit dem Thema umgehen, um so etwas in Zukunft, zumindest in ihrem möglichen Verantwortungsrahmen zu verhindern. Schließlich gibt es ja auch für den Fall eines Brandes in jedem Firmengebäude einen Feuerlöscher und bei jedem größeren Betrieb einen Brandschutzbeauftragen, warum gibt es das noch nicht in jeder Firma im IT-Sicherheitsbereich? Diese Nachlässigkeit bekamen beim „Loveletter“ besonders Bild- und Medienagenturen oder auch andere Firmen, deren Kapital in Bildern steckt, zu spüren, denn der „Loveletter“ löschte sämtliche Bilddateien der Festplatte.

Vorerst nur festzustellen ist die Tatsache, daß 1,5 Monate nach diesem verheerenden Vorfall laut einer Umfrage des Hamburger Forschungs- und Beratungsinstituts MediaTransfer AG lediglich 39,5 Prozent der befragten Unternehmen ihre Sicherheitsvorkehrungen erhöht haben. In knapp 40 Prozent durften und dürfen(?) weiterhin alle Mitarbeiter willkürlich alle E-Mail-Anhänge lesen und öffnen.[3]

Virus : Win32.Hybris
Typ : Wurm
Erstes Auftreten : 25.09.2000
Besonderheiten: verschlüsselt, kann sich von über 70 verschiedenen Sites Komponenten aus dem Web nachladen und bestehende aktualisieren
Verbreitung : sehr hoch, nutzt Winsock.dll zur Verbreitung
Plattform : Win32-Systeme
zstzl. Schadroutine : abhängig von den bis zu 32 verschiedenen installierten Plugins.

Eine nicht zu unterschätzende Gefahr für die computerisierte Welt entsteht durch die sukzessive Abnahme der benötigten Einstiegsintelligenz der Täter. Viren-

Konstruktions-Kits, die frei und für jedermann zugänglich im Internet erreichbar sind, machen es selbst für die, die nicht der Programmierkunst mächtig sind, möglich, einfache Viren zu schreiben. Durch die Nutzung von Hilfsmitteln wie dem „Mutation Engine“ vom „Dark Angel“, ist es auch noch möglich, einfache Viren polymorphisch aufzuwerten .

Mittlerweile ist allein die Zahl der Viren auf über 60.000 angestiegen und täglich gibt es neue Meldungen. Selbst vor PDAs und WAP-Handys macht der Virusbefall keinen Halt. Allerdings ist zu beachten, daß nur ein kleiner Teil der Viren sich wirklich im Umlauf („in the wild“) befindet.

2.1 Malware-Grundlagen

Im folgenden werden die gängigsten Typen von Malware näher und eingehender beschrieben.

Virus

Zur Entstehung des Begriffs Virus vorab ein kurzer chronologischer Abriß der Anfänge:

1980 wurde am Fachbereich Informatik der Universität Dortmund von Jürgen Kraus eine Diplomarbeit mit dem Titel „Selbstreproduktion bei Programmen“ verfaßt. Hier wurde das erste Mal darauf hingewiesen, daß sich unter bestimmten Bedingungen ein Programm wie ein biologischer Virus verhalten kann. Allerdings ging Herr Kraus damals überhaupt nicht auf das Thema IT-Sicherheit ein.

1983/84 wurde von Fred Cohen von der Universität Südkalifornien im Zuge seiner Dissertation „Computer Viruses – Theory and Experiments“ die Theorie von sich selbstreproduzierenden Programmen entwickelt und er trat mit dem ersten selbstgeschriebenen und offiziell bekannt gewordenen Virus auch gleich den Beweis dafür an.

Ein Virus ist also ein Programm mit der Fähigkeit der Selbstreplikation. Zur Reproduktion modifiziert der Virus die zu infizierenden Programme, indem er sich selber in diesen Wirt zusätzlich hineinschreibt. Er hängt sich dabei häufig ans Ende der Datei ran und setzt in die erste Zeile des Wirts einen Sprung an seinen Beginn.

Vorher :

Abbildung 1, „Datei vor der Infizierung

Danach :

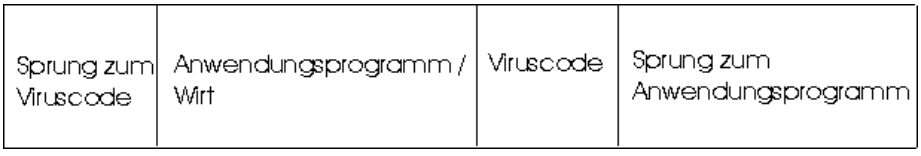

Abbildung 2, „Datei nach der Infizierung“

Wird jetzt der Wirt gestartet, erfolgt auch eine Ausführung des Virus und dieser befällt wiederum weitere Dateien und schreibt sich dort hinein. Also muß der Vi-

rus, bzw. der Wirt, um aktiv werden zu können, ausgeführt werden, daher wird er tunlichst dafür sorgen, sich in ausführbare Dateien zu schreiben (Ausnahme sind die Makro-Viren), wie z.B. *.COM, *.EXE oder *.SYS. Im Gegensatz zu biologischen Viren wird der Wirt also nicht umprogrammiert, um neue Viren zu produzieren, sondern wird lediglich als Träger mißbraucht, der es dem Virus ermöglicht für eine kurze Zeit die Kontrolle über den Prozessor zu erhalten. Viele Viren haben zusätzlich noch eine Schadfunktion (Payload), die zusätzlich zur Selbstreplikation ausgeführt wird. Dieser Wirkteil kann so ziemlich alles enthalten, was den niederträchtigen Gedankengängen der Virenautoren so entspringt. Allerdings gehört diese Schadfunktion laut ursprünglicher Definition von Fred Cohen nicht unbedingt zu einem Virus. In neueren Definitionen eines Virus wird zumindest die böswillige Intention des Autors verlangt.

Ein Virus besteht prinzipiell aus drei Teilen. Der erste Teil übernimmt die Überprüfung, ob eine Datei schon mit dem Virus befallen ist, um eine explosionsartige Vergrößerung der Datei durch erneutes Ranhängen zu verhindern. Der zweite Teil ist der Infektions-/Fortpflanzungsteil, der nach unterschiedlichsten Auswahlkriterien sich seine Opfer aussuchen kann und eventuelle Tarnmechanismen beinhaltet und der dritte Teil beinhaltet den gegebenenfalls vorhandenen Wirkteil.

Nun gibt es verschiedene Typen von Viren. Ein Typus ist der **Bootvirus**. Er befällt keine weiteren Anwendungsprogramme, sondern das System selbst. Er kopiert den originalen Bootsektor auf einen anderen Sektor der Festplatte und markiert den Bereich als „fehlerhaft“. Viele Anwendungsprogramme und damit auch AV-Programme übergehen diese fehlerhaften Sektoren. Nun schreibt er sich selber in den Bootsektor und wird bei jedem Start des Systems ausgeführt. Danach lädt er den originalen Bootsektor.

Ein weiterer Typ ist der **File-, Link- oder Dateivirus**, er verbreitet sich über die ausführbaren Dateien. Wie oben beschrieben wird beim Starten der Wirtsdatei erst der Virus ausgeführt und danach erst die ursprüngliche Datei. Wenn der Virus sich wie in der Grafik gezeigt hinten anhängt nennt man den Virus **„Anhängender Virus“** oder auch **„Appending Virus“**. Eine Alternative dazu stellen der **„Überschreibende Virus“** oder auch **„Overwriting Virus“** dar. Er schreibt sich

einfach über den Anfang der Wirtsdatei und korrumpiert damit den Wirt. Dadurch ist die Gefahr der Entdeckung natürlich wesentlich größer, weil der Anwender schnell bemerkt, daß etwas nicht stimmt, da die Dateien ja nicht mehr ausführbar sind. Um einiges intelligenter sind da Viren, die nach Freiräumen innerhalb der Datei suchen, um sich dort reinschreiben zu können. Das Raffinierte bei diesen **„Cavity-Viren“** ist, daß sie die Größe der Wirtsdatei nicht verändern und damit ein mögliches Erkennungsmerkmal einer Infektion kaschieren.

„Companion Viren“ haben die Eigenart Ihre ursprüngliche Opferdatei unberührt zu lassen und anstelle dessen entweder eine namensgleiche Kopie zur erzeugen, die allerdings statt der befallenen EXE-Datei die Endung *.COM hat, da der Befehlsinterpreter *.COM-Dateien vor *.EXE-Dateien ausführt, oder die zu infizierende Datei bekommt einen neuen Namen und der Virus gibt sich den alten Namen der infizierten Datei. In beiden Fällen wird jeweils zuerst der Virus ausgeführt. Eine weitere Möglichkeit besteht darin, wie beim **„Path-Companion-Virus“** die Tatsache auszunutzen, daß DOS nach einer Datei in der Reihenfolge der Aufführung in der PATH-Umgebungsvariable sucht. Er schreibt sich also unter dem Namen der zu infizierenden Datei in ein Verzeichnis, welches vorher durchsucht wird.

„Multi-Partite-Viren“ oder auch **„Hybrid-Viren“** gehören zu den unangenehmsten Erscheinungsformen, da sie den Bootsektor und ausführbare Dateien infizieren können. Diese Viren sind in der Lage die Stärken der einzelnen Infektion zu kombinieren, indem sie z.B. Tarnungsmechanismen eines **„Boot-Virus“** und gleichzeitig polymorphische Techniken der **„Datei-Viren“** benutzen, um somit ihren Schutz vor Entdeckung zu optimieren. Außerdem haben Sie die Möglichkeit sich zum einen über befallene Dateien durch den **„Datei-Virus“**-Anteil und zum anderen über befallene Dateiträger durch den **„Boot-Virus“**-Anteil zu verbreiten.

„Polymorphische Viren“ ändern ihr Aussehen nach jeder Infektion. Da es eine sehr große Anzahl verschiedener Wege zu einem bestimmten Ergebnis zu kommen gibt (bspw 10=1+4+5 oder 10=8+2 oder 10=1+9), ist es sehr schwierig sie zu erkennen, da man für sie keine eindeutige Signatur haben kann, sondern algorithmisch die Dateien durchsuchen muß.

„FAT-Viren“ oder **„Dateisystem-Viren“** verändern die FAT-Tabelle. In dieser Tabelle stehen die physikalischen Adressen der jeweils gesuchten Dateien. Der Virus kopiert die originalen Adressen auf einen anschließend fehlerhaft markierten Bereich und kopiert seine eigene Adresse in die Tabelle. Wird jetzt eine Datei aufgerufen, deren Adresse in der FAT-Tabelle verändert wurde, dann wird erst der Virus ausgeführt und der schaut danach in die gesicherte Originaladresse, um dann das ursprüngliche Programm ausführen zu lassen.

„Keime/Germs“ sind die „Originalversionen“ der Viren, also die Generation 0, die noch keinen Wirt besetzt hat.

„Makro-Viren“ vermehren sich über den ausführbaren Code, die sogenannten Makros, der in den Dokumenten mancher Anwendungsprogramme wie Word, Excel oder Access steht. Sie erfahren momentan eine sehr große Verbreitung und mit den Skript-Viren aufgrund der einfachen Herstellungsmöglichkeit den größten Zuwachs. Sie infizieren keine ausführbaren Dateien, sondern andere Dokumente. **„Makro-Viren“** klinken sich gerne in das „AutoOpen“-Makro ein, welches beim Start jedes Dokuments ausgeführt wird. Ist erst einmal die „Normal.DOT“ befallen, wird, da sie bei jedem Start von Microsoft Winword als erste ausgeführt wird, automatisch jedes weitere erzeugte Dokument verseucht. Da die Makrosprache nicht nur Formatierungsfunktionen beinhaltet, sondern auch umfangreiche Systemzugriffe damit realisiert werden können, kann auch mit **„Makro-Viren“** nahezu alles gemacht werden, was der Virenautor wünscht.

„Trojanische Pferde“ sind zerstörerische Programme, die neben ihrem destruktiven Anteil zu Tarnungzwecken noch die Erwartungen des Benutzers in das geöffnete Programm erfüllen. Das können z.B. kleine Spiele oder Nutzprogramme sein, die aus dem Internet geladen wurden. Diese „erweiterte Funktionalität“ kann ohne allzu großen Aufwand in das ursprüngliche Programm implementiert werden. Die Schadlast kann sehr unterschiedlich sein, so können z.B. auch Viren oder Würmer in einem **„Trojanischen Pferd“** versteckt sein. Das **„Trojanische Pferd“** selber ist allerdings kein Virus, da es sich nicht selbst fortpflanzt. Ist die Schadlast nun ein Virus und infiziert es nur den Speicher des angegriffenen Systems, nennt man

diese Spezialform auch **„Injector“**, infiziert es auch den Datenträger, nennt man es **„Dropper“.**

„Logische Bomben“ haben sehr viel Ähnlichkeit mit Trojanischen Pferden. Bei **„Logischen Bomben“** gibt es allerdings noch einen Auslöser, eine boolesche Bedingung, die an die Aktivierung der Schadfunktion gekoppelt ist. Ist die Bedingung eine Zeitfunktion, so nennt man diesen Spezialfall auch **„Zeitbombe“**. Im Schnitt werden „**Logische Bomben“** häufig zur Schadensmaximierung eingesetzt. Besonders für frustrierte Arbeitnehmer stellt die **„Logische Bombe“** einen gefährlichen Reiz dar. Eine mögliche Bedingung wäre z.B. die Entfernung des eigenen Namens von der Gehaltsliste einer Firma.

„Würmer“ sind Programme, die für Ihre Ausbreitung keinen Wirt benötigen, sondern sich selber über Netze kopieren. Durch ihre Ausnutzung von Netzwerken können sie eine extrem hohe Ausbreitungsgeschwindigkeit erreichen, was sie besonders gefährlich macht. Es gibt zwei verschiedene Typen von **„Würmern“**, einmal den **„Netzwerk-Wurm“** und einmal den **„Host-Wurm“**. **„Host-Würmer“** bestehen nur aus einem Teil, der komplett auf dem befallenen PC vorhanden ist. Wenn so ein **„Host-Wurm“** nach einer erfolgreichen Ausbreitung seine alte Kopie zerstört, nennt man ihn **„Rabbit“**. Ein **„Netzwerk-Wurm“** besteht aus mehreren Teilen, wobei jeder auf einer unterschiedlichen Maschine läuft. Gibt es eine zentrale Stelle, die die „Arbeit“ koordiniert, nennt man ihn **„Oktopus“.**

„Hoaxes“ sind vorsätzliche Täuschungen mit falschen Meldungen von angeblichen neuen Viren, Würmern oder ähnlichem, welche überwiegend über eMail verbreitet werden. Ziel dieser **„Hoaxes“** ist es, technisch nicht versierte Computernutzer zu verunsichern, zu einer bestimmten Reaktion zu bewegen oder sie sogar in Panik zu versetzen. „**Hoaxes“** gehen immer mit der Aufforderung nach sofortiger Weiterversendung an möglichst alle Bekannten einher.

„Pranks“ sind Programme, die vorgeben etwas Furchtbares zu tun, dieses allerdings nicht auch wirklich machen. **„Pranks“** sind eher als Spaßprogramme zu verstehen, wobei zu bedenken ist, ob es immer noch witzig ist, wenn ein total verstörter Nutzer aus Panik beispielsweise die Festplatte neu formatiert und damit sämtliche Dateien verloren hat. Natürlich können sich solche Programme nicht selbst verbreiten, dann wären es ja auch Viren.

2.2 Aktuelle Virenproblematik

Wir stehen heute vor einer sich verschärfenden Virenproblematik. Die geschätzte Anzahl von existierenden Viren wird zur Zeit auf ca. 60.000 geschätzt. Diese Zahl steigt um geschätzte 5000/p.a., dabei beträgt das Wachstum von Makroviren ca. 25%/p.a. und von Skriptviren ist es sogar >100%/p.a. Diesen Gesamtbestand an Viren, auch Zooviren genannt, steht der Anteil der ITW-Viren gegenüber, ihre Anzahl ist wesentlich geringer, da eine große Anzahl von Viren nur in Laboren oder auf irgendwelchen Web-Servern schlummert oder aber auch einfach nicht „gut“ genug war, um eine größere Verbreitung zu erlangen. Der momentane Stand der am häufigsten vorkommenden Malware kann unter „http://www.wildlist.org“ abgefragt werden.

Das Problem vor dem die AV-Industrie heute steht, ähnelt sehr stark dem Problem der Virologen in der Biologie. Sie kann immer nur reagieren, nicht agieren. Neue Gefahren müssen erst aufgetreten sein, damit sie bekämpft werden können. Aufgrund dieser sehr unangenehmen prophylaktischen Hilflosigkeit ist es umso wichtiger, daß der gemeine Benutzer sensibler mit dieser Gefahr umzugehen lernt, denn nur so kann die Gefahr wirklich kleingehalten werden.

Nicht unerwähnt soll die Tatsache bleiben, daß die AV-Industrie durchaus vor einigen Jahren versuchte prophylaktisch aktiv zu werden; Dateien sollten geimpft werden. Dazu wurden den Dateien die Muster „eingepflanzt“, die die Viren für ihre Selbstüberprüfung nutzten. Wollte ein Virus jetzt eine geimpfte Datei infizieren, wurde er durch die Impfung in der Art und Weise getäuscht, daß er dachte, er hätte die Datei bereits infiziert. Dieses Verfahren hatte aber erdrückende Nachteile. So wurden auch AV-Programme getäuscht, die immer wieder Fehlalarme ausgaben und eine Impfung schloß meistens weitere Impfungen für einen fehlerfreien Betrieb aus. In Anbetracht der großen Anzahl heutiger Viren ist es auch nicht nur unökonomisch, sondern auch einfach nicht realisierbar, jede Datei mit allen Kennungen zu impfen. Des weiteren benutzen heute viele Viren auch andere Mechanismen für ihre Selbstüberprüfung. Heute können Dateien unter die Beobachtung

von Scannern gestellt werden, so daß der Scanner bei einer unerwarteten Veränderung, beispielsweise der Dateigröße, Alarm vor eventuellem Virenbefall schlägt.

Gerade die Mass-Mailer stellen heute ein schwerwiegendes Problem dar. Durch subtilste Art und Weise wird der ahnungslose Anwender dazu gebracht, die „Bombe“ im Anhang zu öffnen. Da wird beispielsweise beim „Naked-Wife“-Wurm der scheinbar frustrierende Vergleich zwischen der eigenen und der fiktiven Frau im Anhang gezogen oder auch eine Variante des weitverbreiteten „Kournikova-Virus“ vom angeblichen Absender „support@t-online.de“, der scheinbar die neue Preisliste von T-Online als Anhang hat.

Der E-Mail-Dienstleister MessageLabs hat bei der Überprüfung von ungefähr 3 Millionen E-Mails pro Tag eine Virusalarmquote von durchschnittlich 1:700 gehabt, also jede 700te E-Mail war im Schnitt verseucht.

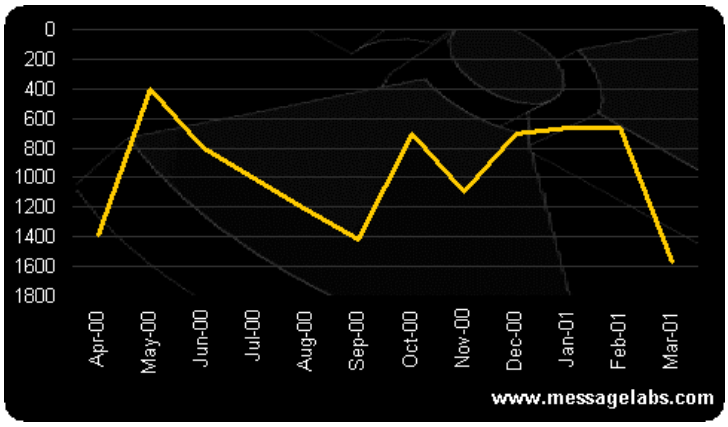

Abbildung 3, „Infektionen von E-Mails (Geprüfte E-Mails/Infektion)“
Copyright 2001, MessageLabs VirusEye, www.messagelabs.com

Die oberste Maxime für Anwender muß es sein, nur angeforderte Anhänge zu öffnen. Für Firmen besteht weiterhin die ego- wie auch altruistische Notwendigkeit, mehr Geld in Sicherheitsschulungen der Mitarbeiter zu stecken. Intervallmäßig stattfindende Informationsschulungen müßten nicht nur zum Aufbau, sondern auch zur Stabilisierung der Sensibilität der Anwender obligatorisch sein. Nur so wird die Firma zum einen ihrer eigenen unternehmerischen Verantwortung gerecht, einen störungsfreien Ablauf zu haben, als zum anderen auch ihrer gesell-

schaftlichen Verantwortung, insbesondere bei MassMailern, nicht als Exponent für die Verbreitung von Malware zu fungieren.

Die benutzten Virentechniken sind größtenteils althergebracht und stellen für die AV-Industrie kein allzu großes Problem mehr dar. Daß aber auch die Virenprogrammierer sich mit neuen Systemen auch neue Gemeinheiten einfallen lassen würden/werden, wurde im Sommer 2000 der AV-Industrie schmerzlich bewußt. Aufbauend auf dem NTFS-Dateisystem von Windows 2000 und Windows NT wurde der erste Streaming-Virus entdeckt. Das Dateisystem NTFS erlaubt es, einzelne Dateien nicht mehr nur wie bei Win9x als einen einzelnen Stream abzuspeichern, sondern sie können über viele verschiedene Streams auf der Festplatte verteilt sein. Das Problem ist, daß momentan die Engines der Antiviren-Produkte nur den Hauptstream nach Viren untersuchen. Wenn der Virus sich also geschickt in die Sub-Streams setzt, wird er von den momentanen Engines nicht erkannt. Glücklicherweise nutzte der aufgetretene W2K.Stream-Virus noch den Hauptstream und konnte somit relativ leicht erkannt werden. Allerdings wird voraussichtlich aus dieser Richtung in nächster Zukunft noch einiges zu hören sein. Eine Umprogrammierung der Engines, so daß auch Sub-Streams untersucht werden, wird nach E. Kaspersky, dem Herausgeber des AV-Produkts AVP, die Scanzeit ca. um ein Drittel verlängern.[4]

Die Schäden, die durch Virenbefall pro anno entstehen, sind mittlerweile enorm hoch und haben eine erschreckende Wachstumsrate. So verbuchte alleine der „Loveletter“ vom Mai 2000 einen geschätzten weltweiten Schaden von über DM 5.000.000.000 für sich. Die Schweizer Rückversicherung Swiss Re ging in einem Rückblick in der 11 Kalenderwoche 2001 in Zürich von einem Schaden von 5,6 Milliarden Mark aus [5]. Weltweit, so schätzt die Hamburger Unternehmensberatung Mummert + Partner, lag der Schaden im Jahr 2000 bei 37,5 Milliarden Mark [6]. Da liegt es nahe, daß die Unternehmen mittlerweile eine berechtigte Angst haben, irgendwann (wieder?) zu den Opfern zu gehören. Nach einer Prognose der Analysten von Frost & Sullivan von Anfang Februar 2001 werden die europäischen Unternehmen in die Internetsicherheit von 525,6 Mill. Dollar im Jahr 2000 auf 3,13 Milliarden Dollar im Jahr 2007 ihre Investitionen aufstocken.

Jedoch wird der Anteil an der Antiviren-Software von 80 Prozent im Jahr 2000 auf 38,5 Prozent im Jahr 2007 sinken. Prozentual stark anwachsen werden die Ausgaben für Content-Filtering und Verschlüsselungstechnologien [7].

In Anbetracht der Schäden, die die Programmierung von Malware verursacht, muß so ein Vergehen auch nicht mehr als Vergehen, sondern mit entsprechend veränderter Strafe, als Verbrechen geahndet werden. Momentan gilt die Programmierung von Malware unverständlicherweise immer noch landläufig eher als Kavaliersdelikt.

Wo über volkswirtschaftliche Schäden, Datenspionage und Verschlüsselung gesprochen wird, darf die USA nicht fehlen. Nachdem sie ohne Rücksicht auf bestehende Verträge und weltweite Kritiken an ihrem Raketenabwehrsystem (NMD) festhalten wollen, fehlt ihnen nur noch ein virtuelles NMD gegen Cyber-Angriffe von außen. Der neue Präsident George W. Bush will dafür in den nächsten Jahren, laut verschiedener Zeitungsberichte, 50 Mrd Dollar freigeben. In wieweit dieses Bestreben Größenwahn ist oder tatsächlich zu realisierende Absichten sind, wird die Zukunft zeigen.

3. Das aVTC

Das aVTC, bis 1998 VTC, ist 1987 von Prof. Dr. Klaus Brunnstein, Dipl. Inform. Wolf-Dieter Jahn und etwa 8 weiteren Studenten, wie beispielsweise M. Swimmer, einem der ersten Programmierer eines Schmalbandantivirus für den Jerusalem-Virus, an der Hamburger Universität, Fachbereich Informatik, gegründet wurden. Die Initiative beruhte unter anderem auf der Entdeckung der ersten Viren, wie dem Brain-Virus 1986, der frühen Erkenntnis, daß die Risiken für die Verbraucher im Zuge dessen stark ansteigen werden und dem Bedarf an IT-Sicherheit-Fachleuten.

Als Ziele hatte sich das aVTC gesetzt, eben diese angesprochenen Fachleute auszubilden, ihnen die Erkennung und Bereinigung von Malware zu lehren und ihnen die dafür benötigten Technologien zu vermitteln. Des weiteren sollte und wurde eine der größten Virendatenbanken weltweit im Zuge der internationalen Kooperation mit CARO aufgebaut. Natürlich ist die Durchführung von Tests per se essentieller Bestandteil des aVTC. Diese Ziele haben sich auch im Laufe der letzten Jahre nicht groß verändert, einzig die Schwerpunktsetzung hat sich verlagert. Es wird mittlerweile mehr Wert auf die Tests als auf die Ausbildung gesetzt, da die angesprochenen Fähigkeiten in anderen parallel laufenden Seminaren, Projekten und Vorlesungen gelehrt werden.

Erstmals vorgestellt wurde das aVTC auf einer Podiumsdiskussion einer Konferenz in Helsinki 1990. Seitdem war es im Expertenbereich ein Begriff, seit 1995/96, dem Zeitpunkt der Veröffentlichung der ersten Tests, auch im Anwenderbereich. Durch die Partizipation von Leuten wie V. Bontchev, einem der führenden Experten im Bereich der Antivirenforschung und –entwicklung weltweit, war von Anfang an eine hohe Reputation gewährleistet.

Die außerordentliche gute Zusammenarbeit mit der AV-Industrie ermöglicht eine sehr gute bilaterale Unterstützung und ist durch den universitären Status des aVTC von eventuellem Mißtrauen wirtschaftlicher Herkunft weitesgehend befreit.

4. Der Anwender

Das schwächste Glied in der Kette bei der Bekämpfung von Malware ist, und bleibt vorerst auch, der Anwender. Die mangelnde Bereitschaft, sich hinreichend über das Thema IT-Sicherheit zu informieren, die fehlende Sensibilität gegenüber möglichen Bedrohungen in scheinbar ungefährlichen Dateien und auf Websites, die vernachlässigte vernünftige Prophylaxe und das fehlende Rechtsbewußtsein des Anwenders sollten unter anderem mithilfe eines Fragebogens (s. Anhang) eingehender untersucht werden und gegebenenfalls bestätigt beziehungsweise widerlegt werden.

Bei Gesprächen mit Anwendern fällt immer wieder das Argument der „belanglosen eigenen Dateien“. Es wäre doch im Prinzip egal, ob damit etwas passiere oder auch nicht. Diese Denkweise muß zwar so erst einmal hingenommen werden, kann und darf aber nicht toleriert werden. Schließlich stellt jeder dieser unachtsamen Anwender eine Gefährdung für die gesamte Netzgemeinschaft dar, da er beispielsweise für Würmer ein weiterer Multiplikator in der Verbreitung, anstatt das Ende eines Verbreitungsastes, wird. Außerdem ist davon auszugehen, das ein Privatanwender, der unachtsam mit seinem Privatcomputer umgeht, keine grundlegend andere Einstellung und Arbeitsweise an seinem Arbeitscomputer zeigen wird.

Hinsichtlich der Tatsache, daß es vielen Anwendern, wahrscheinlich aus fehlender Aufklärung über mögliche Mißbrauchsarten, scheinbar unwichtig ist, was mit der Privatssphäre ihres Computers passiert, muß in der Veränderung dieser Anwenderattitüde einer der Hauptsansatzpunkte eines aktiven Schutzes liegen. Der Anwender verzichtet vorsätzlich auf das Recht einer unberührten Sphäre auf seinem eigenen Computer. Neben der Frage, ob durch die damit moralisch tolerierte Datenspionage und –manipulation auf dem heimischen PC nicht auch ein Bruch mit einem Teil des demokratische Selbstverständnisses einher geht, stellt sich noch die Gefahr des Mißbrauchs des PCs samt seiner Identifikation für weitere Angriffe. So können beispielsweise auf solchen Computern mit beängstigender

Leichtigkeit auch „virtuelle Abschußraketen“ installiert werden, um sie dann mithilfe von kurzen Befehlen von außen für DDos- (Distributed Denial of Service) Attacken zu gebrauchen, wie sie unlängst auf Firmen wie amazon.com niedergegangen sind.

Der erste Schritt muß es sein, dem Anwender das Mystikum Malware näher zu bringen. Sachliche fundierte Aufklärung sollte der erste Schritt sein, um beim Anwender ein grundlegendes Verständnis für die Problematik zu erzeugen. Darauf aufsetzend könnte eine sinnvolle IT-Sicherheit in Firmen aufgebaut werden. Ohne die verstehende(!) Mitarbeit der Angestellten kann aber jedes noch so durchdachte Abwehrsystem ausgehebelt werden. Der Alternative der totalen Rechtebeschränkung und Entmündigung des Anwenders stehen häufig nicht zu letzt auch unternehmerische Gesichtspunkte im Weg.

4.1 Sensibilität für potentielle Gefahren

Häufig ist es so, daß der Anwender hinter vielen Dingen gar keine Gefahr sieht. Dementsprechend wäre es ihm im Prinzip auch nicht zu verübeln, daß er Mails wie den „Loveletter“ öffnet. Nur leider schützt nun einmal Dummheit vor Strafe nicht und die kann leider streckenweise verheerend sein. Das Erreichen einer intelligenten Sensibilität ist also Ausgangsvoraussetzung für jede Schutzmaßnahme. Nun ist dieses Procedere allerdings eine Gratwanderung, denn weder der völlig abgestumpfte Umgang mit Gefahrenpotential noch die Hypersensibilität kann ein gewünschtes Ergebnis sein.

Daß überhaupt eine Gefahr besteht, wollen auch 56 % der befragten Anwender erkannt haben. 27 % sind allerdings der Meinung es gebe zwar eine Gefahr, diese sei aber momentan einfach überschätzt und immerhin 17 % sind überzeugt, daß es überhaupt gar keine Gefahr gebe.

Dementsprechend überrascht es auch nicht, daß 37 % der befragten Personen, die momentane Berichterstattung der Medien als völlig überzogen und für Panikmache halten. Vorgebrachte Argumente sind beispielsweise die Kritik an den Medien, nur über ganz große Angriffe zu berichten und die interessante mehrfach genannte Vermutung, die AV-Industrie selber würde die Panik gezielt anstacheln, um so als Nutznießer höhere Verkaufszahlen zu bekommen. Aber auch bei den 63 %, die die Berichterstattung der Medien begrüßen, gab es Kritik. So wurde das schnelle Akzeptieren der Erklärungen der AV-Industrie, sowie die fehlende Schuldzuweisung an den Nutzer negativ genannt.

Ohne Rücksicht auf eventuelle Sicherheitsbedenken alle Anlagen von e-Mails zu öffnen, gaben 17 % der Befragten zu. Da aber 73 % angaben, sie würden nach bekanntem beziehungsweise unbekanntem Absender unterscheiden, ist bezüglich der Würmer und Mass Mailer, die häufig mit dem Absender ihres letzten, durch das Verschicken an Adreßbuchkontakte ja bekannten Opfers, verschickt werden, kaum von Sicherheitsvorkehrung zu reden. 34 % öffnen immerhin keine Anlagen, die ausführbare Dateien beinhalten. Vielen dürfte aber verborgen sein, daß

beispielsweise auch Makro-Code in Dokumenten und Bildschirmschoner (.SCR) ausführbaren Code darstellen.

Interessant ist in diesem Zusammenhang noch zu bemerken, daß im Gegenzug 83 % der Befragten ohne Bedenken alle Dateitypen übers Netz schicken.

Der Anwender muß diesbezüglich auf die vielen verschiedenen Träger von Malware unbedingt aufgeklärt werden.

Auf die Frage hin, ob denn ihres Ermessens nach, eine Übernahme der Kontrolle über ihren PC von außen, bei einem vorhandenen Internetanschluß, möglich sei, gaben nur 14 % sich selbstsicher, daß so etwas beim besten Willen nicht möglich sei.

4.2 Prophylaxe

Die Prophylaxe, also die Vorbeugung, ist ebenfalls ein ganz wichtiger Punkt beim Thema der Bedrohung durch Malware. Mit entsprechender Vorsorge hätten beispielsweise Würmer wie der „Loveletter“ niemals eine großartige Verbreitung erlangt. Schutzsysteme sind immanent wichtig für ein Computersystem. Da aber täglich neue Viren und andere Bedrohungen entstehen ist es sehr wichtig, daß auch die entsprechenden Abwehrsysteme auf dem neuesten Stand gehalten werden. Ansonsten verlieren diese Systeme logischerweise einen Großteil ihrer Effektivität. Prophylaxe beginnt aber ganz bestimmt nicht bei einem Antiviren-Programm, sondern schon unter anderem bei den Einstellungen des Mail-Klienten und des Browsers. Eine einfache Deinstallation des Windows Script Hosts beispielsweise, den nur die wenigsten Anwender wirklich brauchen, hätte schon viel Schaden verhindern können. Des weiteren gehört aber auch das Schließen von Sicherheitslücken durch Patches der Hersteller des Browsers oder Mail-Klienten dazu.

Immerhin 76 % der befragten Personen gaben an, daß sie ein Schutzprogramm benutzen. Von diesen 76 % war das am häufigsten genutzte AV-Programm der Norton Anti Virus von Symantec mit 53 % und die meistinstallierte Firewall ZoneAlarm mit 26 %. Die meisten nutzen diese Programme auch schon über einige Jahre, aber immerhin 10 % gaben an, aufgrund des „Loveletters“ einen AV-Programm installiert zu haben. Vertrauen in ihr Schutzsystem haben 68 %, während die restlichen 32 % ihrer Abwehr nur gegen die gängigsten Gefahren eine große Chance einräumen.

Geld darf so ein Abwehrsystem natürlich am besten gar nicht kosten. 22 % sind nicht bereit, auch nur ein Pfennig dafür zu bezahlen. Weitere 29 % würden höchstens DM 50,00 investieren. Die nächsten 22 % sehen ihre absolute Schmerzgrenze bei DM 100,00 erreicht. Nur die restlichen 17 % sind bereit für einen umfangreichen Schutz auch tiefer in die Tasche zu greifen. Für bestmöglichen Schutz waren davon sogar 2,5 % bereit bis zu DM 500,00 zu bezahlen.

Wenn es darum geht, ob alles Vertretbare gemacht wurde, sind sich 51 % der Leute sicher, daß sie tatsächlich alles Notwendige für ihren Schutz getan haben. Die anderen 49 % meinten, sie könnten noch weitere und bessere Schutzmaßnahmen treffen. Dazu gehörten beispielsweise die Anschaffung einer Firewall, das häufigere Aktualisieren der Virendefinitionen, das Nutzen eines isolierten Rechners fürs Internet oder die Verwendung von reinen textbasierten Mail-Klienten und Browsern.

Da zu einer vernünftigen Prophylaxe ja wie gesagt auch eine gewisse Sachkenntnis nötig ist, wurden die Leute gefragt, ob bereits eine aktive Informierung über Gefahren und Vorbeugung stattgefunden hat. Immerhin 54 % waren der Meinung dieses hinreichend getan zu haben. Informationsquellen waren dabei zu ungefähr gleichen Teilen, Usergruppen, Offizielle Websites (bspw. von Symantec oder AVP), Mailinglisten, Zeitschriften und/oder „Experten“ aus dem Umfeld.

Nun ist es aber eine Sache, sich einmalig über eine so dynamische Gefahr zu informieren und eine andere Sache, informiert zu bleiben. Immer auf dem neuesten Stand bei Viren-Meldungen sahen sich beispielsweise überraschend hohe 51 %. Für die anderen waren Gründe wie Zeitmangel, fehlendes Interesse, Unverhältnismäßigkeit oder Verzichtbarkeit ausschlaggebend dafür, nicht immer auf dem neuesten Stand zu sein.

Eine relativ große Anzahl von den befragten Leuten hat also Schutzprogramme, ist relativ aktuell informiert und hat ihrer Meinung nach auch alles bezüglich ihrer Sicherheitsvorkehrungen verhältnismäßig zu machende, gemacht. Wird die Software, insbesondere das Antivirenprogramm aber auch regelmäßig genutzt? Da ein On-Access-Scanner häufig entweder nicht installiert oder aus Leistungsgründen deaktiviert ist, ist es besonders interessant zu erfahren, wie häufig denn eine regelmäßige Kontrolle des Systems auf Viren stattfindet. Daß eine Regelmäßigkeit per se besteht, gaben 66 % der Befragten an. Richtig interessant wird es aber erst bei den Intervallen. Von diesen zwei Dritteln gibt es eine tägliche Kontrolle bei 19 %, eine wöchentliche bei 37 %, zweiwöchentlich kontrollieren 22 %, monatlich 11 % und vierteljährlich oder noch seltener kontrollieren ebenfalls 11 %.

4.3 (Un-?) Rechtsbewußtsein

Ein interessantes Phänomen ist das Rechtsbewußtsein des Anwenders. Trotz volkswirtschaftlicher Schäden in Milliardenhöhe wird doch ein Virus häufig eher als natürliches nicht zu verhinderndes Übel angesehen, wofür man streckenweise sogar noch etwas wie Bewunderung empfindet, also für einen vorsätzlich intentional geschriebenen Programmcode, der es darauf abgesehen hat, auf welchem Wege auch immer, Verbreitung und damit Schaden anzurichten. Neben diesem reinen Ressourcenverbrauch haben viele Programme ja sogar wie weiter oben beschrieben noch einen zusätzlichen Schadteil.

Sage und schreibe 37 % der befragten Leute konnten sich sehr gut vorstellen, entsprechendes Wissen vorausgesetzt, einen eigenen Virus zu programmieren. Da liegt es relativ nahe, daß mit 63 % auch fast zwei Drittel, solcher bösartigen Software positive Seiten zuspricht. Der am häufigsten genannte angebliche positive Effekt ist die Verbesserung der Sicherheit der Software. Direkt zu diesem Punkt gab es auch Kommentare von der Seite, die positive Seiten komplett verneint. Sie sehen in der Schaffung von destruktiven Programmen wie Viren zwecks Verbesserung der Sicherheit eine vergleichbar positive Auswirkung wie bei der von Gift. Nämlich die, die Entwicklung von Antiseren zu fördern. Des weiteren sei die Benutzung von AV-Software aufgrund von Viren per se schon negativ, da sie eine Ressourcen- und Geldverschwendung darstellt. Bei den positiven Seiten wurden auch noch Förderung der Programmierkunst des Virenautoren und Rachemöglichkeit genannt. Sehr interessant ist das Argument der Joberhaltung und der Jobbeschaffung auf Seiten der AV-Industrie. Dieser Punkt wurde immerhin von 23 % der Leute genannt, die positive Effekte bei Malware verzeichnen wollen. Zwei weitere sehr interessante Punkte sind einmal das Setzen eines angeblichen Fanals gegen das blinde Vertrauen der Menschen gegenüber Maschinen und zum anderen die scheinbar positive „Lernen-durch-Schmerz“-Methode, den Leuten durch Viren beibringen zu wollen, vorsichtiger zu sein.

Ein wenig konträr zu der Tatsache, daß 37 % Lust hätten, einen eigenen Virus zu schreiben, steht die Tatsache, daß weniger als 5 % angaben, einen Virus jemals

vorsätzlich weitergegeben zu haben. Scheinbar scheint weniger die Schädigung als die einfache Lust am Programmieren von etwas „Besonderem“ vorrangig zu sein.

Bei den Gründen für das Programmieren von Viren gibt es eine ganze Reihe von verschiedenen Ideen, welcher Punkt der Ausschlaggebende ist. Die drei meisten Gründe waren Langeweile, Technisches Wissen unter Beweis stellen und der Machtbeweis mit jeweils ungefähr 27 % (Mehrfachnennungen waren natürlich möglich). Auf den Plätzen ohne Reiheinfolge kommen Industriespionage, Asozialität, Terrorismus, Profitgier, Spaß, Verlust von ethischem Gefühl, besondere Ethik, Herausforderung, mangelnde Anerkennung in der Gesellschaft, Anarchismus, Zerstörungswut, Niederträchtigkeit, Neugierde, Hobby und das Aufzeigen von Lücken. Besonders interessant war wiederum die Vermutung, die AV-Industrie selber schreibe diese Viren oder gebe sie zumindest in Auftrag.

Bei der Bestrafung sind sich wieder alle einig – Virenautoren müssen bestraft werden. Nur 3 % sind der Meinung, daß eine Bestrafung völlig unnötig sei. 41 % der Befragten verlangen eine harte Bestrafung der Virenschreiber incl. Schadensersatzzahlung soweit wie möglich und langjährige Haftstrafen. In 4 % der Fälle wurde sogar explizit verlangt sämtliche Folgen zu tragen. Dazu gehöre auch, im Falle eines Verlustes von beispielsweise medizinischen Akten, aus dessen Folge heraus ein Patient stirbt, die Bestrafung nach zumindest fahrlässiger Tötung.

5. Der aVTC-Wintertest 2000/2001

Bevor auf die Testergebnisse per se eingegangen wird, soll das Testverfahren kurz skizziert werden.

Nachdem die Entscheidung für einen neuen Test gefallen ist, wird im Rahmen des Projektseminars „Aktuelle Probleme der IT- und Netzsicherheit“ unter Leitung von Prof. Dr. Klaus Brunnstein, ein Termin gesetzt, zu dem die Scanner von den Firmen eingereicht sein müssen. Die Firmen werden angeschrieben und es wird Ihnen angeboten, Ihre Scanner einzusenden. Die Datenbanken werden zu diesem Zeitpunkt eingefroren, das heißt es werden keine neuen Virensamples in diese Testdatenbanken aufgenommen, um den AV-Herstellern eine vernünftige Zeit (einige Wochen) einzuräumen, in der sie ihre Scanner auf den neuesten Stand bringen können. Parallel werden die Datenbanken vorbereitet, das heißt die gesamten zugeschickten und gesammelten Virensamples werden kategorisiert und gesondert abgelegt. Problematisch ist hierbei, daß aufgrund individueller Namenvergabe der Einsender die einzelnen Dateien größtenteils manuell angeschaut werden müssen, um sie einem bestimmten Typus zuordnen zu können. Mit 3-4 Scannern, die in den letzten Tests durchweg auf Spitzenplätzen landeten, wird der sogenannte Vortest gemacht. Dabei überprüfen die Scanner die komplette Datenbank. Eine Datei, die von keinem Virusscanner als Malware identifiziert wurde, wird vorerst aus dem Test herausgenommen und später überprüft, ob hierbei wirklich Malware vorliegt. Danach beginnt erst der eigentliche Test nach dessen Abschluß noch die umfangreiche Auswertung steht. Die Auswertung umfaßt umfangreiche Statistiken, Grafiken und Konklusionen. Sie wird nach Abschluß auf der Website des AGN „http://agn-www.informatik.uni-hamburg.de“ zum Herunterladen zur Verfügugung gestellt Die nicht erkannten Samples eines Virenscanners werden den Herstellern zur Aufnahme in ihre Virenscanner zur Verfügung gestellt.

Bei dem aktuellen Test, dem aVTC-Wintertest 2000/2001, wurden die Betriebssysteme DOS, Windows 98, Windows 2000, Windows NT und Linux getest. Linux war hierbei zum ersten Mal vertreten. Die für den Test erstellten Datenbanken, die die Scanner überprüfen müssen, sind : File, File ITW, Boot, Boot ITW, File-Malware, Polymorphisch, Virenkit, Makro, Makro Malware, Makro ITW, Skript, Skript ITW, Exot, Gepackt Makro und Gepackt File.

Als sehr zeitaufwendig stellt sich bei jedem Test aufs neue die Datenbankvorbereitung raus, die sich aufgrund der manuellen Dateiüberprüfung bei vielen der über 150.000 Dateien verständlicherweise als sehr zeitintensiv erweist. Eine normierte Dateibezeichnung würde die Vorbereitung stark verringern. Ein weiteres Problem stellt die nur stark begrenzt zur Verfügung stehende Hardware dar. Bei der großen Menge von verschiedenen Datenbanken, Betriebssystemen und Scannern, sind die für manche Betriebssysteme bereitgestellten 2 PCs einfach zu wenig. Allerdings kann ein hervorragendes Team so einiges kompensieren.

Da leider der Test nicht rechtzeitig fertig wurde, können die Resultate nicht in dieser Arbeit beschrieben und aufgeführt werden..

6. Minimieren Institutionen wie das aVTC die Bedrohung ?

Es gibt eine ganze Reihe von verschiedenen Websites, Institutionen, Selbsthilfegruppen, Pseudoexperten und Fachleuten, die sich auf Ihre Fahnen geschrieben haben, die Gefahr durch Malware zu verringern und zu bekämpfen. Interessant ist aber im Endeffekt das, was aus den ganzen Bemühungen an Fortschritten und Verbesserungen resultiert.

Nüchtern betrachtet sehen wir momentan einen rasanten Anstieg von Malware, einen völlig unzureichend aufgeklärten Anwender, eine ungeklärte Rechtslage, eine stark herabgesetzte Einstiegsintelligenz durch Malwaregeneratoren für Virenprogrammierer und eine zwangsweise auf Reaktion und damit Schadensbegrenzung beschränkte AV-Industrie. Nicht unbedingt ein Zustand, der als befriedigend angesehen werden kann.

Das aVTC in Hamburg stellt von seinen Fähigkeiten ein Kompetenzzentrum dar, welches aber weit unter seinen Möglichkeiten agiert. Der durchschnittlich halbjährlich durchgeführte Test von Antiviren-Produkten ist auf jeden Fall erst einmal ein schönes kostenloses Ranking für die Industrie, welches bei gutem Abschneiden auch hervorragend PR-mäßig gebraucht werden kann, aber inwieweit beeinflußt es die Bedrohung durch Malware? Sicherlich, die Weitergabe der nicht gefundenen Virensamples an die betreffenden Hersteller oder die Empfehlung auch virenfremde Malware wie Trojaner endlich in die Schutzprogramme aufzunehmen sind auf jeden Fall positive Beiträge, aber das Potential ist um ein Vielfaches größer.

Eines der Hauptprobleme liegt doch darin, daß der Anwender nicht vernünftig und verantwortungsvoll mit seinen Daten und seinem Computer umgeht. Warum setzt man nicht hier an und versucht den Kreis der elitären Eingeweihten aufzusprengen und das Gros mit notwendiger Information zu versorgen?! Gesammelte Erfahrungen, wie die auf der Messe „Hamburger Computer Tage“ haben gezeigt, daß gerade dort großer Handlungsbedarf ist. Handzettel mit checklistenartig aufgebauten

einfachen Informationen zur Überprüfung beziehungsweise Verbesserung des Systems wurden mehr als nur dankbar aufgenommen. Institutionen wie das aVTC haben den Vorteil der Befreiung von notwendiger wirtschaftlicher Vorteilsnahme. Der Kunde braucht auch keine Angst vor irgendwelchen finanziell orientierten Hintertürchen zu haben. Auf der anderen Seite kann das aVTC weitere Kompetenzen aufbauen und sich vom Antiviren-Spezialisten zum Sicherheitsspezialisten im Gesamtbereich Malware-Behandlung ausbauen. Studenten könnten beispielsweise auf der aVTC-eigenen Website Foren führen, Informationsbibliotheken aufbauen und Sicherheitsüberprüfungssysteme installieren. Dafür sollten neben Studenten aus Projekten auch Studentische Hilfskräfte benutzt werden, die aus der Wirtschaft gesponsert werden müßten. In der Mannstärke liegt auch tatsächlich das größte Problem. Ein Ausbau der Aufgaben und Ziele geht natürlich nur mit einer Vergrößerung des aVTC an sich einher. Ein enges Zusammenarbeiten mit den Medien ist ebenfalls notwendig. Die letzten Jahre haben gezeigt, daß großangelegte Medienberichte immer wieder die Sensibilität steigern konnten.

Bezüglich des Tests bietet sich ein Gütesiegel an. Hierzu sollten die führenden akzeptierten Testzentren weltweit sich zusammenschließen und ein Kriterienkatalog zur Vergabe des Siegels ausarbeiten. Es darf nicht sein, daß teilweise AV-Produkte, die signifikante Schwächen in der Erkennung und Beseitigung von Malware aufzeigen, nur aufgrund von gutem Marketing hohe Verkaufszahlen erreichen. Die Folge davon sind zu Unrecht beruhigte Anwender, die im Falle einer Infektion häufig nur unzureichende Schutzvorkehrungen haben. Hierbei entsteht volkswirtschaftlicher Schaden, der nicht zu akzeptieren ist. Die Folge eines solchen Siegels wären auf jeden Fall erhöhter Leistungsdruck, Wettbewerb und ganz entscheidend eine verbesserte Einflußnahme von nicht wirtschaftlichen Interessen. Ziel muß es sein, eine Etablierung des Siegels zu erreichen, daß es „nicht gut ist, es zu haben, sondern schlecht, es nicht zu haben“. Hier bietet sich wiederum ein Miteinander mit den Medien an. Durch enge gemeinschaftliche Zusammenarbeit kann so auf diesem Gebiet eine Effizienzverbesserung im Bereich der AV-Software erreicht werden.

Projekte wie der „Malware-Crawler“ von Sönke Freitag, der die automatische Durchforstung des Internets nach Malware vornehmen soll, zeigen, daß es aufgrund der vorhandenen Kompetenzen durchaus möglich ist, neben dem Test per se auch noch Konzepte und Ideen zu entwickeln, die ebenfalls einen nicht unerheblichen Beitrag zur Bedrohungsverkleinerung abliefern können. Denkbar wäre hier auch die Programmierung eines Plug-In, welches eine datenbankgesteuerte Schwarze Liste beinhaltet, in der malwarelastige Websites aufgeführt werden. Der Anwender könnte somit vor Betreten einer derartigen Site einen Warnhinweis bekommen. Nicht abzustreiten ist allerdings auch die Gefahr, daß die Schwarze Liste für manche eher attraktiv als abschreckend wirkt und solchen Leuten sogar die Suche nach diesen Sites abgenommen werden würde, sie hätten sogar den Vorteil einer ständig aktualisierten Liste. Für die Verjährung der Einträge bietet sich beispielsweise eine Variante des Verebbungsalgorithmuses an. Das aVTC sollte versuchen, ihren Testbestandteil, absolut gesehen, nicht zu verringern, aber ihn anteilsmäßig gleichberechtigt neben Zielen wie der Funktion als Informationsquelle für Anwender, Steigerung der Sensibilität der Anwender und Förderung des Prophylaxeverhaltens zu stellen. Durch den verstärkten Kontakt mit Anwendern und damit der permanenten Problemzuführung würde das aVTC direkt am Puls der Sicherheitsprobleme stehen und könnte neben der markt- und problemkonformen Bearbeitung neuer Projekte, Informatiker aus der Uni entlassen, die neben theoretischem Hintergrund auch noch permanenten Kontakt mit aktuellen Problemen und Erfordernissen des Marktes hatten. Das aVTC und damit das Informatikum und Hamburg hätten aufgrund der hervorragenden Ausgangsbedingungen die Möglichkeit, eine Schmiede für Sicherheitsexperten zu werden. Aufgrund der Tragweite sind politische und wirtschaftliche Unterstützung selbstverständlich unabdingbar, denn nur so kann der notwendige Bedarf an zusätzlichen Kräften auch durchgesetzt werden.

Um insgesamt ein ausgewogenes Meinungsbild zu bekommen, wurde neben dem Fragebogen an Anwender auch einer an die AV-Industrie (s.Anhang) geschrieben. Einige Erkenntnisse daraus werden im folgenden dargestellt.

So wird mehr oder weniger unisono von den Befragten unter anderem das Zusenden der nicht erkannten Virensamples gelobt. Durch diese Tatsache kann neben dem eventuellen Werbeeffekt auch eine signifikante Verbesserung ihres Scanners als Ergebnis aus dem Test gezogen werden. Die Verwendung aus werbewirksamen Gründen ist per se ja auch völlig in Ordnung und fast wünschenswert, schließlich kann nur bei guten Leistungen, das Testergebnis für die Werbung benutzt werden und gute Leistungen sind wiederum gut für den Anwender. Bei bekannten Tests ist sogar die Teilnahme fast obligatorisch, wie streckenweise erwähnt wurde, da ein Fernbleiben jedes Mal in irritierten Anrufen endet, die erklärt haben wollen, warum der Scanner nicht partizipiert habe.

Das aVTC wurde für seine Professionalität hoch gelobt, was besonders erwähnenswert ist, da die meisten Tests in den Augen der Befragten stümperhaft und unprofessionell durchgeführt werden. Neben dem aVTC wurde auch mehrfach positiv das Virus Bulletin und die Universität Tampere genannt.

Dem aVTC wird von Seiten der AV-Industrie eine direkte Wirkung auf Entwicklung und Produktion der Scanner zugesprochen. Was allerdings immer wieder störend erwähnt wird, ist die lange Testdauer, die manche Ergebnisse, einfach durch eine mittlerweile durchgeführte Korrektur, als veraltet stehen lassen.

7. Zusammenfassung & Ausblick

Die Ausgangsfrage neben der Darstellung des Wintertests war, inwieweit Institutionen wie insbesondere das aVTC in Hamburg, Auswirkungen auf die Bedrohung der computerisierten Welt durch Malware haben. In der Summe hat das aVTC auf jeden Fall eine Auswirkung, die sich insbesondere auf folgende Fakten stützt: Verbesserung der AV-Software durch Tests, Hinweise und Zusendung verpaßter Virensamples, Ausbildung von angehenden AV-Experten, Bereitstellung der Ergebnisse der breiten Masse auf der Website mit der Folge einer „intelligenten“ Produktwahl für den Anwender und die Funktion als Ansprechpartner bei Problemen mit Malware. Wie in Kapitel 6 ausführlich konstatiert, ist das Potential des aVTCs aber bei weitem größer.

Der Anwender hat sich als völlig unzureichend informiert und unsensibel gegenüber potentiellen Gefahrenträgern aber mit überraschend relativ hohem grundlegenden Prophylaxeverhalten, also der Nutzung eines AV-Programms, herausgestellt. Das Rechtsbewußtsein ist eher als doppelzüngig einzustufen, es besteht einerseits die Erwartung an die Gerichte und die Justiz, Autoren solcher Malware hart zu bestrafen, auf der anderen Seite existiert ein erschreckend hohes Interesse daran, selber Autor zu werden, wenn auch aus den Antworten vermutet werden kann, daß es um die reine Programmierung nicht um die Verbreitung geht.

Vorsichtig die Zukunft einschätzend ist zu sagen, daß damit gerechnet werden muß, daß die Verbreitung und Bedrohung durch Malware weiter stark ansteigen wird, die AV-Industrie auf unbestimmte Zeit auf Reaktion beschränkt sein wird, der Anwender bei gleichbleibendem Desinteresse und Unterschätzung der Gefahr keine signifikant andere Einstellung und Verbesserung seiner Arbeitsweise zeigen wird und das das aVTC weiter hervorragende Tests machen wird, aber aufgrund fehlender politischer und wirtschaftlicher Unterstützung es schwer haben wird, einen größeren Stellenwert bei der Bekämpfung einzunehmen.

8. Anhang

Im folgenden finden Sie einmal den verschickten Fragebogen an die AV-Industrie und zum anderen den Fragebogen an die Anwender. Die AV-Industrie wurde direkt, bzw. über das aVTC-Forum angeschrieben und um die Beantwortung gebeten. Der Bogen für Anwender wurde über private Kontakte und Newsgroupanfragen verteilt.

Fragebogen an die AV-Industrie:

You have participated (are participating) in VTC tests.

Concerning arguments and reasons

Your general assessment about threats of a) self-replicating and b) non-self-replicating malware ?

1.1 Why do you participate ?
(e.g. quality control, quality comparison, good PR, to avoid bad PR,...)

1.2 Do you regularly participate in any other tests? If yes, in which ?

1.3 What is your general opinion on such tests ?

1.4 How important is the economic interest for participating in a test ?

1.5 Would you take part in tests if you had to pay a fee ?

Concerning management of test participation

2 How do you prepare for a test?

2.1 Do test results have a direct effect on your development/production? Why and if yes, how ?

2.2 Would you say, that test results and therefore the test, made a contribution to improve the quality of your product?

Concerning VTC tests

3 How do you prepare for a VTC test (if there are any differences from 2) ?

3.1 Are VTC reports fairly judging the quality of your product ?

3.2 Did it help you to improve your products by receiving the missed samples? How important is it for you to get them ?

3.3 Is there something in VTC tests which you find superfluous ?

General Aspects

4. Do you think that it will get better or worse in the near future? Why?

4.1 What worries you about the Internet the most?

4.2 How do you judge the user?

4.3 Has the way the Internet is being used by the user got better or worse? Why?

4.4 What would you expect of the user?

4.5 Do politicians/does the law deal with virus programmes and their contamination in the right/wrong way? Why?

4.6 Do you think that the AV industry will ever be in control of the situation? Why?

4.7 Did the test draw your attention to complications, which you did not recognise or perhaps did not consider to be important?

4.8 Do you see national differences in the virus problem? Why?

Fragebogen an die Anwender:

1) Nutzen Sie Programme, um sich vor Gefahren wie Viren oder Angriffen zu schützen ? Wenn ja, um welche Art von Programmen handelt es sich?

2) Seit wann nutzen Sie solche Programme ? Gab' es einen bestimmten Grund dafür ?

3) Haben Sie Vertrauen in diese Programme ? Fühlen Sie sich damit sicher ? Warum ?

4) Denken Sie, es gibt momentan eine akute Gefahr durch bösartige Software wie Viren ? Wie hoch schätzen Sie sie ein ?

5) Sind Sie schon einmal Opfer von solcher bösartigen Software geworden ? Wenn ja, von welcher und welchen Schaden hatten Sie ?

6) Halten sie die in letzter Zeit häufig gebrachten Berichte der Medien über Gefahren aus dem Netz und durch Software für überzogen und Panikmache ? Warum ?

7) Könnten sie sich vorstellen, entsprechendes Wissen vorausgesetzt, selber einen Virus zu programmieren ?

8) Finden Sie, daß es auch positive Seiten von solcher bösartigen Software gibt ? Wenn ja, welche ?

9) Haben Sie schon einmal vorsätzlich einen Virus weitergegeben, aus welchem Grund auch immer ?

10) Wieviel sind Sie pro Jahr bereit, für Ihren Schutz vor solchen Angriffen auszugeben ?

11) Denken Sie, daß Sie alles notwendige für Ihren Schutz vor solchen Angriffen tun ? Wenn ja, was ? Wenn nein, was könnten Sie noch machen ?

12) Öffnen Sie alle Anlagen, die Ihnen geschickt werden ? Wenn nein, wonach unterscheiden Sie ?

13) Können Sie sich vorstellen, daß jemand von außen, einen Internet-Anschluß vorausgesetzt, die Kontrolle über Ihren PC übernehmen kann?

14) Schicken Sie Anlagen jeden Typs übers Internet ? Wenn nein, welche nicht ?

15) Haben Sie sich schon einmal fachkundig über die Gefahren und mögliche Vorsorge informiert ? Wenn ja, wo bzw. bei wem ?

16) Sind Sie, was Viren-Meldungen betrifft immer auf den neuesten Stand oder legen Sie keinen Wert darauf ? Wenn ja, wie schaffen Sie das ? Wenn nein, warum nicht ?

17) Nutzen Sie ICQ ?

18) Untersuchen Sie in regelmäßigen Abständen Ihr System auf Viren ? Wenn ja, in welchen ?

19) Warum denken Sie, schreibt jemand bösartige Software ?

20) Denken Sie solche Leute sollten (leicht/hart/überhaupt nicht) bestraft werden ? Warum ?

9. Literatur- und Quellenverzeichnis

[1] w3.zdf.msnbc.de/news/36038.asp „Viren verursachen Milliardenschaden“, 2000

[2] www.internetworld.de/5tage_3289.html „Umfrage: Ist Microsoft am Virus-Gau schuld ?“, 09.05.2001

[3] www.golem.de/0006/8334.html „Deutsche Unternehmen vernachlässigen Si cherheitsmaßnahmen“, 22.06.2000

[4] www.tecchannel.de/software/541/index.html „Neuer Virus unterläuft alle Vi renscanner“

[5] Hamburger Abendblatt „Teurer Computervirus“, 16.03.01

[6] Hamburger Abendblatt „Milliardenschäden durch Viren“, 24/25.03.01

[7] www.internetworld.de/sixcms/detail.php?id=7698, „Prognose: Virenschutz wird sekundär“, 06.02.01