

Thematik: Anti-Malware-Systeme: Viren, Würmer und trojanische Pferde
Aufgabe: Einblick in Anti-Malware-Systeme und deren lokalen und zentralen Lösungen

Referenten: Sebastian Spooren < nws@spooren.de >
Timm Kruse < techt@gmx.de >

Lehrveranstaltung: Informatik, Netzwerksicherheit (NWS-A)

Dozent: Prof. Dr. Norbert Pohlmann

Ort, Datum: Fachhochschule Gelsenkirchen, 06.12.2004

1	Definition von den Begrifflichkeiten	Seite
1.1	Malware	3
1.2	Viren	3
1.3	Würmer	5
1.4	Trojanische Pferde	5
2	Historie	
2.1	Warum alles begann	6
2.2	Wie alles begann	6
3	Verbreitungswege	
3.1	Verbreitung über E-Mail & Applikationen	8
3.2	Ausnutzung von Sicherheitslücken in Applikationen	8
4	Identifizierung	
4.1	Allgemeines	10
4.2	Spezielle Verfahren	10
4.3	Heuristische Verfahren	10
4.4	Integritätsprüfer	11
4.5	Emulatoren	11
4.6	Einsatz der Verfahren	11
4.7	Geschwindigkeit von Virensclannern	12
4.8	Wie werden neue Viren-Signaturen erstellt?	12
4.9	Die Indizien für ein Virus	12
4.10	F-Prot – Virensignatur vom 23.11.2004	13
5	Beseitigung	
5.1	Entfernung von Viren	13
5.2	Removal-Tools	13
5.3	Harter Kampf bei Symantec	14
6	Lokale und Zentrale Schutzmöglichkeiten vor Malware	
6.1	Allgemeines	14
6.2	Zentrale Schutzmöglichkeiten	14
6.3	Lokaler Schutz	15
6.4	Sicherheitsvorkehrungen	15
7	Bekanntes & aktuelle Meldungen aus dem Malware-Bereich	
7.1	Persönliche Erfahrung im IT-Bereich	16
7.2	Details zum Wurm: W32.Blaster	17
7.3	Details zum Wurm: W32.Sasser	18
7.4	Details zum Wurm: W32.Mydoom	18
7.5	Details zum Wurm: W32.Bagle	19
7.6	Details zum Wurm: W32.Sober Variante Sober.I	20
8	Zukunftsperspektiven	
8.1	Gegenwart	20
8.2	Viren und Spam: Bedrohung in E-Mails	21
8.3	Virenbedrohung allgemein	21
8.4	Potentielle Bedrohungen durch Mobilität in den Griff bekommen	21
8.5	„Code-Check-Tools“ – Das Ende der Sicherheitslücken und Buffer Overflows?	21
8.6	Schlusswort	22
9	Gespräch mit Sophos	22
10	Literatur- und Quellangaben	24

1. Definition von den Begrifflichkeiten

Malware

Malware bedeutet, wie das Wort „Mal“ schon suggeriert, schlechte Ware. Konkret steht Malware für *Malicious Software* und heißt soviel wie böswillige Software. Unter dem Aspekt Malware fallen Viren, Würmer, trojanische Pferde, Dialer, Spyware, Hoaxes und andere Arten gefährlicher Software.

Malware wird einerseits von versierten Programmierern erstellt, um gezielt Schaden anzurichten. Diese Personen kommen nur vereinzelt vor und verfügen meistens über eine besonders gute Betriebssystem-Sachkenntnis. Allerdings entstehen *täglich* neue Virenvarianten mit unterschiedlichen Aktionen, die Überlebenscharakter im WWW haben und nicht von den oben genannten Spezialisten erstellt worden sind. Die meisten Viren sind nur kleine modifizierte Weiterentwicklungen von Computerfreaks, die meistens einer Community angehören. Des Weiteren kommen so genannte *Virengeneratoren* zum Einsatz, mit denen ohne Programmierkenntnisse Viren oder auch Trojaner erstellt werden können.

Viren

Viren wird meistens als Oberbegriff der Malware benutzt (bspw. Anti-Viren-Software), obwohl sie spezielle Eigenschaften gegenüber anderen Computer-Schädlingen haben. Viren verbreiten sich innerhalb eines PCs und infizieren Datei für Datei. Würmer hingegen nutzen die Infrastruktur eines Netzwerkes (LAN / verteilte Systeme wie das WWW) und Trojaner tarnen sich als nützliche Tools.

Viren nutzen die Autorisierung von Programmen im Betriebssystem und sind *keine selbständigen Programmroutinen*, sondern integrieren ihren Programmcode in Dateien (bspw. auch in Bilder).

Ähnlich dem HI-Virus der vom Immunsystem (unserem Anti-Viren-Programm) nicht erkannt wird, weil sich das Virus in einer körpereigenen Zelle befindet. Weitere Parallelen zur biologischen Gattung folgen gleich.

Es ist daher insbesondere sehr gefährlich, wenn Viren Anti-Viren-Programme befallen haben (bspw. Sober.I der einige Anti-Viren-Programme deaktiviert). Um hier vorzubeugen unterziehen sich die Anti-Viren-Programme beim Start auch stets einem Selbsttest mit dem Vergleich von vorher erzeugten Prüfsummen (Dateigröße, Erstellungsdatum, Prüfzahl vom Inhalt der Datei). Raffinierte Viren können sich Anti-Viren-Programmen gegenüber unsichtbar verhalten (*Stealth-Viren*), da sie sich bei einem Virens캔 vorübergehend in den Arbeitsspeicher auslagern und nach der Dateiüberprüfung wieder in den Programmcode einschleusen. Viren geben sich i.d.R. nicht zu erkennen, sondern versuchen mit Tarntechniken im Hintergrund aktiv zu bleiben und sich zu *verbreiten* (sei dies in Form von Datenträgern, Netzwerken, Dateien im gleichen Dateisystem). Die Ausführung der Schadensfunktion erfolgt i.d.R. erst, wenn eine bestimmte Bedingung eingetreten ist, die sicherstellt, dass das Virus sich genügend verbreitet hat. Erst dann, aufgrund eingeschränkter Sicherheitskriterien, wird das Virus in den meisten Fällen vom Benutzer entdeckt (siehe Identifizierung) – doch dann ist es oft schon zu spät.

Warum die Schädlinge eigentlich Viren heißen wurde schon anhand des HI-Virus deutlich. Hier noch weitere Parallelen mit dem biologischen Namensvetter:

- Viren sind sehr klein und blockieren i.d.R. vitale / systemnahe Funktionen.
- Ein Virus haftet sich an einen Wirt und schleust seine virenspezifischen Gene / Programmcode ins Zellinnere bzw. in die Software und missbraucht dann die betroffene Zelle / den Prozess für seine weitere Verbreitung.

- Wie bei den biologischen Viren sind viele Computerviren mutiert. Sie unterscheiden sich meistens nur in den Aktionen (Bsp. Hepatitis A/B/C). Es ist daher immer eine Herausforderung für Anti-Viren-Programme, solche Mutationen zwecks intelligenter Heuristik-Methoden und Signatur-Verfahren weitestgehend zu erkennen.

Virenarten

Vorab sei gesagt, dass man zwischen Viren in freier Wildbahn und sog. Zooviren unterscheidet. Nur etwa *1 bis 2 Prozent* aller bekannten Viren sind tatsächlich auf Computern in aller Welt *aktiv* und werden in regelmäßigen Abständen von der WildList-Organisation dokumentiert.

siehe <http://www.wildlist.org>

- **Bootviren** befinden sich nach Infizierung im Bootsektor des Systems. Sie kommen seltener vor, sind aber im Gegensatz zu anderen Virenarten *zerstörerischer*. Ihr systemnaher Bezug erleichtert die *zuverlässige Ausführung*.
- **Dateiviren** infizieren ausführbare Dateien und *replizieren sich* beim erneuten Aktivieren des betroffenen Prozesses.
Es gibt anhängende Viren, die sich an das Ende eines Programms hängen, aber noch eine Zeile am Anfang des Programmcodes für die Sprungadresse schreiben. Hierbei funktioniert der alte Programmcode weiterhin und das Virus wird i.d.R. daher vom Benutzer nicht schnell erkannt.
Bei einer anderen Methode ersetzt das Virus das Wirtsprogramm in Teilen oder vollständig, was zur Folge hat, dass dieses unbrauchbar und der Schaden in den meisten Fällen schnell entdeckt wird.
Eine ausgeklügelte Variante stellen so genannte „Cavity-Viren“ dar. Sie suchen im Programmcode nach unbenutzten Freiräumen, wo sie ihren Code einbetten können. Auch Fragment-Techniken der Viren sind hier denkbar. Die Wirtsdateien verändern bei dieser Methode nicht ihre Länge und Dateigröße und stellen Virenschaltern demgegenüber wieder ein weiteres Hindernis dar (aber dafür gibt es Checksummen und Signaturen).
- **Polymorphe Viren** verwenden nach einer Programminfektion verschiedene Mechanismen, um ihren *Programmcode* zu *modifizieren* bzw. zu *verschlüsseln*; somit werden sie von Anti-Viren-Programmen anhand ihrer Signaturen nicht erkannt. Dies können einfache Mechanismen wie die Ersetzung von a+b zu b+a sein oder das Hinzufügen von nutzlosen Befehlen, um der Signaturerkennung des Virenschalters entgegen zu wirken.
- **Stealth-Viren** sind spezielle *Tarnviren*. Sie entfernen ihren Code aus einer infizierten Datei, sobald diese von einem Anti-Viren-Programm geöffnet und analysiert wird. Nachdem ein Anti-Viren-Programm die Datei durchsucht hat (und keinen Virus finden konnte) wird die Datei erneut vom Stealth-Virus befallen.
- **Makroviren** werden auch als sehr gefährlich eingestuft (vermehrt nach Einführung von Microsoft Windows 95), da diese mit relativ einfachen Programmierkenntnissen erstellt werden und erhebliche Schäden anrichten können. Ihr Schaden wirkt sich dennoch i.a. nur auf Dokumentendateien wie bspw. Word und Excel aus. Dennoch ist es mittels Makros möglich eine Menge der Systemkomponenten anzusprechen und Kommandos auszuführen. Inwieweit die Lauffähigkeit von Makros gewährleistet ist, hängt u.a. auch vom Betriebssystem ab.
- **Multipartite-Viren** sind in der Lage Datei- und Bootsektor-Records anzugreifen

Würmer

Würmer benötigen kein extra Wirtsprogramm, wie dies bei Viren der Fall ist. Sie sind kleine eigenständige Prozesse und benutzen gerne systemhomonyme Prozessnamen (siehe Wurm „MyDoom“). Würmer nutzen Schwachstellen in Netzwerken aus, um sich zu vervielfältigen und sich nicht auf isolierten Rechnern zu verbreiten. Sie dringen in den Speicher eines Rechners ein und ermitteln Netzwerk- und E-Mail Adressen um sich weiter auszubreiten. Die Gefahr liegt in ihrer rasanten Ausbreitungsgeschwindigkeit, die nur durch automatische Mechanismen wie Firewall-Systeme verhindert werden kann. Bei Erkennung durch den Benutzer sind bereits zahlreiche Rechner infiziert. Würmer treten daher oft auf, wenn Sicherheitslücken in Systemen ausgenutzt werden (bekannte Methoden sind so genannte „Buffer Overflows“). Böswillige Aktionen der Würmer lassen Schäden in Millionen-, sogar Milliarden-Höhe entstehen. Die exponentiell steigende Netzauslastung, bei voller Infizierung aller im Netz beteiligten Rechner, legt schnell große Netzwerke lahm.

Bekanntes Beispiel aus den Medien:

Melissa: Infiziert innerhalb von drei Tagen 100.000 Rechnersysteme

Der große Erfolg von Computerwürmern sind die besseren „Lebensbedingungen“. Ein Sicherheitsexperte der Firma Symantec: „Für den Loveletter dürften das Microsoft-Handbuch, ein Nachmittag und eine ordentliche Portion kriminelle Energie genügt haben, um einen Schaden von geschätzten 2,5 Milliarden Dollar weltweit anzurichten.“ Dies liegt an dem enormen Wachstum von vernetzten Computern im WWW, welche potentielle Angreifer oder Opfer von Computerviren darstellen bzw. an dem rasanten Wachstum der Computerindustrie mit der Partizipierung in fast jeder Arbeitsbranche.

Trojanische Pferde verbergen hinter einem Programm, wie z.B. einem Spiel, gefährlichen Programmcode. Der Begriff stammt vom „Hölzernen Pferd“ (griechische Sage Troja – der Film sicherlich einigen bekannt). Der Aktivierungszeitpunkt ist unbekannt (solche Malware wird auch als logische Bombe deklariert). Das heißt also auch, dass Trojaner Viren oder Würmer beinhalten können. Wobei das Ziel hier meist das Ausspähen von Daten ist.

Sie besitzen i.d.R. keine eigenständigen Verbreitungsroutinen. Trojaner machen sich im Gegensatz zu trojanischen Pferden nicht die Mühe und täuschen ein normales Programm vor. Ein Trojaner besteht aus zwei eigenständigen Programmen (Server/Client).

Eine besonders aggressive Form des trojanischen Pferdes sind so genannte Backdoor-Trojaner. Diese richten auf dem Wirtssystem Ports (Backdoors) ein, durch die ein Hacker via Fernzugriff auf den Rechner zugreifen kann, um sich gezielt Informationen zu beschaffen. Mit Hilfe von Backdoor-Trojanern wie bspw. Netbus, SubSeven und BackOrifice kann der Hacker auf fremde Rechner zugreifen und über Fernkontrolle beliebige Funktionen ausführen.

Die Anzahl von professionellen Trojanern ist in den vergangenen Jahren gestiegen, da Betriebssysteme aufgrund der Weiterentwicklungen, wie bspw. Active-X, immer wieder neue Sicherheitslücken aufweisen. Die Motivation bei Betrügnern besteht darin sicherheitsrelevante Daten wie Passwörter, die z.B. beim Online-Banking benötigt werden, auszuspähen.

2. Historie

Warum alles begann

In den meisten Fällen geht es den Viren-Programmierern um Anerkennung in einer Community oder einfach darum anderen Schaden zuzufügen. Manchen geht es auch darum monopolistischen Unternehmen wie Microsoft darauf aufmerksam zu machen, dass sie verwundbar sind und dass ihre Systeme nicht perfekt sind (bspw.: VBS.Monopoly der auf die Monopolstellung der Firma Microsoft hinweist).

Wie alles begann

Mit der Revolution der Computer - immer leistungsstärker - ist auch die Entwicklung der Malware nicht stehen geblieben. Jeden Tag stehen neue Virendefinitionslisten durch Anti-Viren-Updates zur Verfügung. Das Internet fungiert inzwischen als äußerst nahrhafter Boden für Malware, da nahezu jeder einzelne im Internet partizipierte Computer ein potentieller Wirt sein kann und mit Millionen von Computern weltweit vernetzt ist.

1982	entstand das erste Virus (Typ: Bootvirus) namens „Elk Cloner“ außerhalb eines akademischen Labors. Das Virus benutzte das Betriebssystem zur Verbreitung über Disketten. Mitarbeiter bei Xerox entwickelten Programme, die sie für verteilte Rechenoperationen im Netzwerk einsetzen wollten. Diese gerieten allerdings außer Kontrolle, sodass viele Rechner neu gestartet werden mussten - <i>der Anfang der Computerwürmer</i> .
1986	kam dann der erste PC-Virus „Brain“ aus Pakistan (Typ: Bootvirus mit Tarntechniken) erster Datei-Virus „Virdem“ aus Deutschland
1987	Viren verbreiten sich weltweit an Universitäten (bbspw. Stoned-Virus aus Wellington)
1988	gab es dann den ersten Anti-Virus-Virus aus Indonesien der den Brain entfernte. 10% (6000) der im Internet befindlichen Rechner wurden mit einem Internetwurm befallen.
1989	ging die Weiterentwicklung von Viren erst so richtig voran erster schnell infizierender Virus „Dark Avenger.1800“ aus Bulgarien
1991	Symantec bringt als Vorreiter die erste Sicherheitssoftware gegen Malware auf den Markt – viele andere Hersteller folgen schnell. Paradoxerweise: Veröffentlichung des ersten Virus-Construction-Sets.
1992	Inzwischen existieren schon über 2000 verschiedene Viren weltweit <i>Michelangelo's</i> Ziel: am 06. März alle Computersysteme runterfahren Dark Avenger veröffentlicht „Mutation Engine“ zur automatischen Erzeugung von polymorphen Viren.
1993	Anti-Virus-Industrie veröffentlicht ihre erste Wild-List.

1995	wird Black Baron (britischer Staatsbürger) wg. Computerkriminalität in 11 Fällen zu 18 Monaten Haft verurteilt. Mit der Einführung von Windows 95 entstehen viele Makroviren.
1998	W95.CIH-Virus aus Taiwan überschreibt BIOS
1999	Melissa verbreitet sich sehr schnell an bis zu 50 Adressen aus Outlook und infiziert Word-Dokumente. Der Massenversand führt zum Absturz vieler Mailserver. Es wird versucht Netbus 2 Pro als kommerzielles Programm zu legalisieren, um vor Virenschaltern gezwungenermaßen unentdeckt zu bleiben.
2000	Ähnlich wie Melissa verbreitet sich der Loveletter rasend schnell und bringt zahlreiche Mailserver zum Absturz und verursacht nach Schätzungen einen Schaden in Höhe von 9 Milliarden US\$ (8x soviel wie Melissa) erster Trojaner für PDA's verbreitet sich über SYNC-Mechanismus
2001	Besonders gefährlich: W32/Naked – getarnt als Flash-Animation verschickt er sich an alle Outlook-Kontakte und erfordert, aufgrund der Löschung von Systemverzeichnissen, eine Neuinstallation des Systems. Der als besonders aggressiv eingestufte, äußerst komplexe Computerwurm Nimda manipuliert sogar Webserver und nutzt neben dem Verbreitungsmechanismus E-Mail nahezu 20 Schwachstellen des Betriebssystems Windows aus. W32/BadTrans galt bis dato als verbreitetester Virus weltweit, da es unbeantwortete E-Mails zitiert, auf den Anhang verweist und an den entsprechenden Absender verschickt. Er spioniert mit Hilfe eines KeyLoggers Passwörter aus.
2002	W32/Bugbear: erster Wurm mit eigener SMTP-Engine verbreitet sich sehr schnell.
2003	Der SQL-Slammer wird einstimmig von allen Viren-Experten als schnellster Wurm bezeichnet – binnen Minuten verbreitet er sich, aufgrund einer implementierten Endlosschleife für Neu-Infizierungen, weltweit rasant aus. Er beeinträchtigte den gesamten Internetverkehr immens. Es bleibt weiterhin ungeklärt ob der SQL-Slammer für den größten Stromausfall der US-Geschichte (50 Mio. Menschen ohne Strom) verantwortlich war. Hinweis: Auszug aktueller Malware-Meldungen im Detail unter Punkt 7

3. Verbreitungswege

Verbreitung über E-Mail & Applikationen

Viren greifen Dateien an. Wird eine befallene Datei ausgeführt, so infiziert das Virus, aufgrund des wiederholenden Prozesses, Datei für Datei.

Die häufigste Verbreitung findet über den E-Mail-Verkehr statt. Das Virus wird als Dateianhang verschickt und mit einem Begleittext versehen. Dieser Text soll einen dazu bewegen, den Dateianhang auszuführen und somit den eigenen Rechner zu infizieren. Das Gleiche gilt auch für Nachrichten in Newsgroups. In einigen Fällen handelt es sich um eine Virenwarnung, wobei die ausführbare Datei im Anhang als Sicherheitsupdate bezeichnet wird. Daher besteht Gefahr bei unwissenden Anwendern.

Ein auch sehr häufiger Verbreitungsweg findet über illegale Kopien von Anwendungen und Spielen statt. In Zeiten von High-Speed-Verbindungen (DSL) werden die illegalen Kopien über Tauschbörsen bezogen und gelangen hierdurch auf den heimischen Rechner. Kleine Software-Applikationen, die man sich im Internet downloaden kann, können von Viren befallen sein (Moorhuhn: mehrere Varianten mit Trojanischen Pferden bekannt). Dieses Sicherheitsrisiko ist bei größeren Anbietern, wie Chip.de oder Download.com, wesentlich geringer als bei kleinen privaten Internet-Seiten. Des Weiteren ist auf illegalen Warez-Seiten, oder jenen die Netzwerktools wie Port-Scanner und Key-Logger anbieten, häufig mit einer infizierten Datei zu rechnen.

Makroviren verbreiten sich bspw. über Word-Dokumente. Sie befallen die übergeordneten Dokumentenvorlagen und beschädigen somit jedes Dokument, das mit Word geöffnet wird. Allein der Zugriff auf ein Word-Dokument mit einem Browser, der einen Viewer als PlugIn benutzt, reicht für eine Infizierung aus.

Ausnutzung von Sicherheitslücken in Applikationen

Ein sehr ernstzunehmender, und vor allem nie komplett einzudämmender Verbreitungsweg, ist das Ausnutzen von Sicherheitslöchern in Standardsoftware. Alleine das Betriebssystem Windows hat eine Vielzahl von Sicherheitslöchern (bspw. Betrachten von JPEG´s, LSASS ausgenutzt von Sasser). Gerade ist ein Sicherheitsloch gestopft, werden schon wieder neue entdeckt, so dass Programmierer mit notwendigen Updates gar nicht mithalten können. Dies erklärt, warum es für viele bekannte Sicherheitslücken noch keine Updates gibt. Aber nicht nur Windows, sondern auch andere Softwareprodukte, sind von Sicherheitslücken betroffen (Internet Explorer, Apache Server, Microsoft Internet Information Server).

Test der Sicherheit des eigenen Browsers auf Heise:

<http://www.heise.de/security/dienste/browsercheck>

Benutzt man einen Rechner ohne eingespielte Updates und Firewall mit einer Verbindung zum Internet, so wie es heute noch sehr oft der Fall ist, ist man den Würmern hilflos ausgeliefert. Der Rechner empfängt ständig Anfragen an einem offenen Port, über den sich Würmer in das System einschleusen. Z.B. Port 445, der für den Datenaustausch im Netzwerk zuständig ist. Ist der Port offen schleust sich Code in den Rechner ein und lädt den eigentlichen Wurm von bereits infizierten Rechnern nach. Dafür startet er auf einem weiteren Port einen FTP-Server. Der befallene Rechner führt nun selbst Anfragen an andere Rechner aus und versucht diese zu infizieren. Man kann sich denken, dass sich ein Wurm sehr schnell verbreitet, da viele Systeme im Internet die gleichen Sicherheitslücken haben.

Grafik: Blockierte Zugriffe auf Port 445 von ZoneAlarm

Date / Time	Type	Protocol	P	Source IP	Destination IP ▾	Direction
2004/11/24 15:08:42+1:00 GMT	Firewall	TCP (flags:S)		80.143.124.191:4586	192.168.1.1:445	Incoming
2004/11/24 15:08:34+1:00 GMT	Firewall	TCP (flags:S)		80.143.61.52:3910	192.168.1.1:445	Incoming
2004/11/24 15:04:30+1:00 GMT	Firewall	TCP (flags:S)		80.143.170.112:3152	192.168.1.1:445	Incoming
2004/11/24 15:02:02+1:00 GMT	Firewall	TCP (flags:S)		80.143.176.58:4650	192.168.1.1:445	Incoming
2004/11/24 15:01:56+1:00 GMT	Firewall	TCP (flags:S)		80.143.65.186:4217	192.168.1.1:445	Incoming
2004/11/24 15:00:38+1:00 GMT	Firewall	TCP (flags:S)		80.143.189.6:4649	192.168.1.1:445	Incoming
2004/11/24 14:58:26+1:00 GMT	Firewall	TCP (flags:S)		80.143.57.36:1571	192.168.1.1:445	Incoming
2004/11/24 14:58:12+1:00 GMT	Firewall	TCP (flags:S)		80.143.165.36:4827	192.168.1.1:445	Incoming
2004/11/24 14:57:42+1:00 GMT	Firewall	TCP (flags:S)		80.143.228.220:1029	192.168.1.1:445	Incoming
2004/11/24 14:57:24+1:00 GMT	Firewall	TCP (flags:S)		80.143.145.149:1118	192.168.1.1:445	Incoming
2004/11/24 14:57:24+1:00 GMT	Firewall	TCP (flags:S)		80.143.226.241:4265	192.168.1.1:445	Incoming
2004/11/24 14:56:40+1:00 GMT	Firewall	TCP (flags:S)		80.143.61.53:1386	192.168.1.1:445	Incoming
2004/11/24 14:54:50+1:00 GMT	Firewall	TCP (flags:S)		80.143.237.73:4532	192.168.1.1:445	Incoming
2004/11/24 14:54:40+1:00 GMT	Firewall	TCP (flags:S)		80.143.124.240:4033	192.168.1.1:445	Incoming
2004/11/24 14:54:28+1:00 GMT	Firewall	TCP (flags:S)		80.143.170.112:4173	192.168.1.1:445	Incoming
2004/11/24 14:51:40+1:00 GMT	Firewall	TCP (flags:S)		80.143.145.149:1114	192.168.1.1:445	Incoming

Exploits dienen der Demonstration einer Sicherheitslücke und sollen den Softwarehersteller dazu zwingen schnell ein Update zu programmieren, das die Sicherheitslücke stopft. Durch die Exploits sind auch einfache Programmierer in der Lage eine Sicherheitslücke auszunutzen und Schadsoftware zu schreiben. Entdecker der Sicherheitslücken verheimlichen diese vor der Öffentlichkeit und geben Firmen somit Zeit diese zu schließen, bevor sie damit an die Öffentlichkeit gehen.

Es gibt Fälle, bei denen sog. Spammer in Zusammenhang mit Würmern stehen. Die Würmer öffnen den Spammern Tür und Angel, indem sie einen SMTP-Server auf dem lokalen System starten, der dann ungehindert Spam versenden kann.

Auch größere Firmen sind nicht vollständig geschützt, indem sie auf ihrem Server, der das ganze Netzwerk mit dem Internet verbindet, eine Firewall und einen Virenschanner in Betrieb haben. Denn jeder Mitarbeiter der ein Notebook besitzt und dieses auch außerhalb der Firma nutzt, kann so einen Wurm in das Netzwerk einschleusen.

Viren und Würmer finden eine immer stärker werdende Verbreitung und somit war es nur eine Frage der Zeit, wann die ersten Viren für Handys auftauchen. Ein Beispiel ist der sich seit Juni 2004 im Umlauf befindliche Virus „Cabir“. Er infiziert Handys mit dem Symbian System, das eine große Bluetooth-Sicherheitslücke hat. Er verbreitet sich von Handy zu Handy, in dem er über Bluetooth nach anderen Geräten sucht. So ist es möglich das Hacker via Laptop oder PDA auf verschiedene Handy-Modelle zugreifen und kostenpflichtige Telefonate an 0190-Nummern ausführen.

Je mehr Rechner zum lokalen Netzwerk oder Internet gehören, umso schneller können sich Würmer, Viren und Trojaner ausbreiten. Beispiele für Verbreitungsgeschwindigkeiten folgen. Netzwerke sind ihr Lebensraum und die Gefahr ist umso größer wenn standardisierte Software eingesetzt wird.

Zu den Anfängen der Malware waren nur bestimmte Regionen betroffen, da der größte Verbreitungsweg über Disketten vonstatten ging. Weltumspannende Netze, wie das Internet, ermöglichen heute eine rasante interkontinentale Verbreitung.

Identifizierung

Allgemeines

Zu Beginn der ersten Anti-Viren-Programme wurden ausführbare Dateien komplett nach einem bestimmten, nämlich vom Virus abhängigen Teilcode (im weiteren Verlauf Such-String genannt, engl. „Search String“) durchsucht. Man erkannte nach einiger Zeit, dass das Virus relevanten Coden an den Anfang einer Datei schreibt und konnte somit die Suche effizienter gestalten und sich auf Teile des Dokuments beschränken. Durch die Veränderung der Betriebssysteme und der immer neueren Varianten von Viren und Würmern hat sich die Technologie von Anti-Viren-Software in den letzten Jahren deutlich geändert. Es wurden immer nur Dateien gescannt, aber es tauchten Viren auf, die auch ohne Dateien existieren konnten; wie z.B. Skriptviren, die erst beim Zugriff einer E-Mail aktiviert wurden.

Erst nachdem das Skript ausgeführt wird kann der Virens Scanner das Virus überhaupt finden, vorher ist es für ihn unsichtbar.

An Skriptviren ist das Gefährliche, dass der Quellcode gleich mitgeliefert wird. Jede kleinste Veränderung bedeutet eine neue Variante. Somit wird es künftig immer wichtiger für Virens Scanner polymorphe Viren aufzuspüren, die nur kleine unbedeutende Änderungen mit sich bringen. Der Wurm Phatbot bspw. verschickt seinen eigenen Quellcode als Anhang per E-Mail. Somit ist es auch für unerfahrene Programmierer ein Leichtes, Änderungen vorzunehmen und in Umlauf zu bringen.

Anti-Viren-Software wird immer komplexer, um neue und immer raffinierter werdende Viren zu entdecken.

Spezielle Verfahren

Dateien werden nach einem individuellen Erkennungsmuster durchsucht, die typische Merkmale für ein Virus sind. Sollte der Such-String auch zufällig in einer gewöhnlichen Datei vorkommen, so schlägt auch hier der Virens Scanner fälschlicherweise Alarm. Wird ein bekanntes Virus in kleinen unbedeutenden Teilen verändert und betrifft die Änderung nur teilweise den bekannten Such-String, so versagt die spezielle Suche und kann das Virus nicht mehr identifizieren. Somit ist jede noch so kleine Variante eines bekannten Virus unauffindbar, bis die Virendefinition aktualisiert wird. Um Virens Scanner nicht so einfach zu umgehen, braucht man heute andere Verfahren. Die speziellen Suchmethoden sind besonders gut geeignet um bestimmte Viren zu entdecken und über diese detaillierte Informationen zu liefern.

Heuristische Verfahren

Als immer mehr Viren in Umlauf kamen, dachte man daran effektivere Scanner zu entwickeln, welche neue, unbekannte Viren aufspüren. Es gibt grundsätzlich zwei Methoden die diese neue Suche realisieren.

Einerseits kann man nach allgemeinen Such-Strings suchen, die Viren standardmäßig beinhalten. Untersucht man Viren genauer, so stellt man fest, dass sich bestimmte Programmier Techniken wiederholen, die Viren zur Verbreitung einsetzen. Allerdings gibt es keinen einzigen Programmierbefehl, bei dem sichergestellt ist, dass es sich hierbei zu 100% um ein Virus handelt.

Andererseits kann man anhand von Regeln Programmzugriffe überwachen. Jeder Programmzugriff wird überprüft und nach festgelegten Kriterien bewertet. Wird nun das Sicherheitsrisiko einer Datei als hoch bewertet, so ist anzunehmen, dass es sich hierbei um ein Virus handelt. Das Zugreifen eines Programms auf das Adressbuch von Outlook ist ein solches Kriterium (andere sind das Kopieren von Makros in Dokumentenvorlagen, das Verschieben oder Kopieren von Programmcode im Arbeitsspeicher oder Schreibzugriffe auf den Bootsektor der Festplatte).

Trojaner sind schwieriger zu erkennen, da sie keine Verbreitungsroutine besitzen und daher eher als ein „normales“ Programm eingestuft werden. Man kann sie nur

entdecken, wenn man ihre Versuche zur Tarnung näher betrachtet. Heuristische Methoden stoßen aber auch an ihre Grenzen; denn die Merkmale stützen sich eben nur auf Vermutungen. Es können nicht alle neuen Viren und Würmer erkannt werden, denn schließlich werden nur bekannte Heuristiken verwendet. Nutzt ein Virus eine neue Taktik, entgeht er dem Virens Scanner. Daher wird bei einer Vermutung auf einen Virus oder Wurm auch nur die Meldung „Virusverdacht“ ausgegeben und nicht „Virus gefunden“. Heuristische Verfahren haben den Vorteil *neue* Varianten zu identifizieren. Sie können aber im Gegensatz zu den spez. Suchmethoden keine bestimmten Informationen ausgeben.

Integritätsprüfer

Hierbei wird anhand der Prüfsumme validiert, ob sich eine Datei seit dem letzten Zugriff verändert hat. Die Prüfsumme ist leicht zu fälschen, weshalb man auf CRC und MD5 Verfahren setzt. Der Trick dabei ist, dass alle Dateien, die sich seit dem letzten Scanvorgang nicht verändert haben, nicht noch mal mit allen Identifizierungsmethoden überprüft werden müssen, sondern nur die Prüfsummen. Hat sich vorher kein Virus in der Datei versteckt, so ist anzunehmen, falls sich die Dateigröße nicht verändert hat, dass auch dann kein Virus enthalten ist. Der Nachteil: War eine Datei vor der Integritätsprüfung schon befallen, ändert sich die Prüfsumme nicht und es wird kein Verdacht geschöpft. Manche Viren versuchen die vorhandenen Prüfdaten einfach zu löschen, um somit eine Prüfung zu verhindern, daher muss der Integritätsprüfer sich selbst vor Manipulationen schützen.

Emulatoren

Als besonders kompliziert erweisen sich polymorphe und verschlüsselte Viren. Sie verschlüsseln sich immer wieder mit einem neuen Schlüssel und anderen Verfahren. Dadurch ist es fast unmöglich den Virus zu entdecken, da er immer eine andere Gestalt annimmt. Aber auch hier gibt es ein Verfahren, um auch diese Arten zu erkennen. Man emuliert sie, um Informationen über ihre Auswirkung und Techniken zu erhalten. Die Programmierer der Anti-Viren-Programme lassen diese Viren in einer sicheren Umgebung laufen. Nachdem sie sich kurzzeitig entschlüsselt haben, führen sie ihre Funktionen aus. Die nötige Entschlüsselungsmethode enthält das Virus direkt selber, da er sonst nie zur Ausführung käme. Da Virenautoren sich immer neue Tricks einfallen lassen, wird hierbei vom raffinierten Virus geprüft, ob er wirklich auf einem „normalen System“ läuft und nicht nur in einer simulierten Umgebung. Daher müssen die Virenspezialisten bestimmte Vorkehrungen treffen, damit sich das Virus richtig entfaltet.

Einsatz der Verfahren

Einen guten Virens Scanner macht nun die perfekte Kombination aller Methoden aus, um einen effektiven Schutz zu gewährleisten. Der Unterschied zwischen normalen Anwendungen und Trojanern oder Viren ist nur sehr klein, wodurch sie alten Suchmethoden häufig entgehen. Dem entgegengesetzt verbrauchen die heuristischen Verfahren viele System-Ressourcen und beeinträchtigen die Performance des Systems und stören damit den Benutzer bei seiner täglichen Arbeit. Zudem können sie unerwünschte Falschmeldungen liefern.

Testen kann man einen guten Virens Scanner am besten, indem man die Virendatenbank nicht aktualisiert und diesen dann Dateien mit neueren Viren überprüfen lässt. Im besten Falle sollte er Alarm schlagen und den Virus entfernen können.

Aber auch Virens Scanner, die sämtliche Virenarten auf Anhieb finden, nützen nur wenig, wenn sie nicht schnell arbeiten und dem Benutzer nur unnötig Rechenzeit verwehren.

Geschwindigkeit von Virenschannern

Um Geschwindigkeit einzusparen sollte die Virendatenbank sortiert sein, damit ein schneller Zugriff auf die verschiedenen Virenarten möglich ist. Es macht auch keinen Sinn, im Hauptspeicher des Rechners nach Makroviren zu suchen, da diese sich nur in Dateien verbergen. Der Zugriff auf die zu prüfenden Dateien sollte schnell vonstatten gehen wobei nur der nötigste Teil einer Datei gescannt wird. Etwa die Hälfte der Zeit, die ein Scannvorgang braucht, entspricht dabei dem Zugriff auf Dateien der Festplatte. Wächterprogramme überwachen die Programme bei Ausführung. Die meisten Virenschanner haben diese Funktion als Hintergrundprozess implementiert. Bei jeder Programmausführung läuft somit erst der Hintergrundprozess ab, bevor das eigentliche Programm gestartet wird. Dies geht auch zu Lasten der Geschwindigkeit.

Wie werden neue Viren-Signaturen erstellt?

Ein neues Virus taucht normalerweise nicht als erstes bei den Spezialisten auf, die für die Erstellung neuer Signaturen zuständig sind. Somit müssen die Programmierer erst einmal an das neue Virus gelangen, um es zu analysieren. Dies geschieht in der Regel von Kunden der Anti-Viren-Software über Einsendungen an das Anti-Viren-Labor. Hätte man nur einen Virenschanner laufen, würde man keine neuen Virenarten entdecken, da diese von dem Scanner nicht gefunden würden. Also müssen zusätzliche Tools zur Untersuchung herangezogen werden. Z.B. Monitoring-Tools, die den Zugriff auf jeglichen Speicher überwachen und beim Zugriff auf diesen Meldungen ausgeben.

Ist ein Virus erst einmal gefunden, werden verschiedenste Tests durchgeführt und der Such-String bestimmt. Zirka 90 Prozent aller Einsendungen werden vollautomatisch einer Analyse unterzogen. Handelt es sich bei der Analyse um ein neues Virus, erstellt das System in über 70 Prozent aller Fälle automatisch die Signatur und das Gegenmittel und informiert den Absender mit dem Gegenmittel als Attachment. Da der Prozess vollkommen automatisch abläuft, funktioniert der Vorgang auch an Feiertagen, nachts und während Urlaubszeiten ohne Verzögerung. Die Analyse und Erstellung der Signatur sowie des Gegenmittels dauert i.d.R. etwa 40 Minuten (bei bekannten Viren: 10 Sekunden).

Für Anti-Viren-Hersteller ist es unmöglich alle Virenarten zu dokumentieren. Daher werden nur die wichtigsten und am weitest verbreitetsten Viren sorgfältig analysiert.

Handelt es sich um ein polymorphes Virus, so kann man nicht einfach einen Such-String definieren, sondern muss selbst speziellen Code schreiben, um das Virus ausfindig zu machen. Dies ist nur in wenigen Fällen notwendig. Hierbei muss auf Spezialisten zurückgegriffen werden. Wenn eine Datei nicht automatisch analysiert werden kann, erhält der zuständige Virenexperte einen Hinweis. Je nach Komplexität dauert das bei Makroviren gerade mal 10 Minuten und bei komplexen Viren bis zu einer Stunde. Loveletter war so ein Fall. Hier dauerte es eine Stunde, den Virus zu analysieren.

Die Zeitspanne, in der Viren-Signaturen heutzutage erstellt werden, wird immer kürzer. Es vergeht nicht ein Tag, an dem eine neue Definitionsliste erstellt wird. Deshalb wird in Zukunft das Thema Virenschanner immer eine große Bedeutung haben.

Die Indizien für ein Virus

Möchte man als Anwender selber überprüfen, ob sich ein Wurm auf dem eigenen System befindet, so sollte man sich als erstes die Autostart-Einträge angucken, denn ein Wurm aktiviert sich schließlich bei jedem Systemstart neu. Am einfachsten ist dabei der Zugang zum Autostart-Ordner, aber am wirkungsvollsten sind die Autostart-Einträge in der Registry. Es gibt aber auch noch andere Systemdateien, in denen Startanweisungen für Programme beim Systemstart stehen, wie bspw. „win.ini“, „system.ini“. Es erweist sich auch als hilfreich, die aktiven Prozesse zu überwachen

und systemhomonymen Prozessnamen auf die Spur zu kommen. Über den Befehl „netstat“ kann man sich direkt aktive Verbindungen von Netzwerk und Internet ausgeben lassen.

Weitere Indizien sind:

- Dateilänge hat sich verändert
- Absturz nach Ausführung eines sonst stabilen Programms
- häufige Festplattenaktivität, obwohl kein Programm aktiv ist, unter der Voraussetzung, dass Hintergrundprogramme wie Scheduler deaktiviert sind
- veränderte Dateieigenschaften
- seltsame Bildschirmmeldungen

F-Prot – Virensignatur vom 23.11.2004

Malware-Typ	Anzahl
DOS/Windows	59.975
Unix/Linux	409
Makro (Office)	8.283
Java	245
PalmOS	4
Script (VB, JavaScript, Unix Shell, IRC, INF)	7.657
Batch und andere (AMi, PIF, PHP, WinBAT, BAT)	2.957
Zerstörende Programme	55.405
insgesamt Viren, Würmer, Trojaner und Backdoors	134.935

4. Beseitigung

Entfernung der Viren

Wenn Virens Scanner auf eine infizierte Datei treffen, sollte diese sofort desinfiziert werden. Bekommt der Benutzer nur eine Warnmeldung, so müsste er sich noch um die explizite Entfernung kümmern. Die beste Entfernung wäre, wenn man die Datei löschen würde und von einer Sicherungskopie die Datei wieder rekonstruiert. Aber nur in den seltensten Fällen existieren Sicherheitskopien und sind zudem auf dem neusten Stand, so dass wirklich keine Daten verloren gehen würden. Benutzerfreundlicher scheint der heute standardisierte Weg, dass Virens Scanner die Datei direkt vom Virus befreien, um ein sicheres Weiterarbeiten zu ermöglichen. Die Erkennung und Beseitigung finden vom selben Programm statt.

Aber wie entfernt man ein Virus? Es ist nicht damit getan, dass Virens Scanner den Prozess, zu der die ausgeführte Datei gehört, stoppt. Das System würde zwar weiterarbeiten, allerdings wäre die Ursache des Fehlers nicht behoben. Die meisten Virens Scanner heutzutage enthalten Funktionen zum Löschen von Malware. Dies geschieht, indem der schädliche Code aus der Datei und eventuell Registry-Einträge entfernt werden. Doch nicht immer lässt sich ein Virus leicht aus einer Datei entfernen, ohne dabei Daten zu zerstören. Es gibt viele Viren, bei denen das Reparieren nicht möglich ist, weil z.B. ein Teil der Datei von diesem überschrieben wurde.

Removal-Tools

Ist der eigene Rechner schon von einem Wurm befallen und hat der Virens Scanner diesen nicht erkannt, so hilft ein spezielles Removal-Tool. Diese Tools gibt es für bekannte Würmer kostenlos bei den Anti-Viren-Programmherstellern im Internet. Die Programme sind so ausgerichtet, dass sie nur einen bestimmten Wurm entfernen

können. Das setzt voraus, dass man weiß, um welchen Wurm es sich beim befallenen Rechner handelt.

Kennt man den Wurm nicht, kann man auf Programme zurückgreifen, die speziell nach Würmern suchen und diese entfernen. Ein Beispiel ist hierfür das kostenlose Programm „Stinger“ von der Firma McAfee. Es erkennt und entfernt die häufigsten Würmer, Viren und Trojaner. Bei Erscheinung eines neuen gefährlichen Schädlings wird das Programm um Mechanismen erweitert, um auch diesen erfolgreich zu bekämpfen. Da insbesondere Würmer Sicherheitslücken in Anwendungsprogrammen oder im Betriebssystem ausnutzen, sollten diese nach Entfernung des Wurmes durch Sicherheits-Updates geschlossen werden.

Für versierte Computernutzer stellen die Sicherheitsfirmen auch Informationen über die manuelle Entfernung bereit. Eine „Schritt für Schritt-Anleitung“ gibt Hilfestellung bei der Entfernung ohne ein spezielles Tool. Dabei müssen mit großer Wahrscheinlichkeit Registry-Einträge geändert oder komplett entfernt werden.

Harter Kampf bei Symantec

Der härteste Kampf, um ein Gegenmittel gegen einen Wurm zu finden, war laut Symantec Ende 1998. Der Wurm „RemoteExplore“ ist ein sehr komplexes Programm, das aller Wahrscheinlichkeit nach von einem sehr guten Programmierer erstellt wurde. Die Mitarbeiter benötigten für die Analyse einen vollen Tag, wobei die Erstellung des Gegenmittels einige Tage in Anspruch nahm. Das Virus ist glücklicherweise nicht weit verbreitet.

5. Lokale und Zentrale Schutzmöglichkeiten vor Malware

Allgemeines

Selbst die teuerste und noch so gute Technik liefert keinen 100%igen Schutz vor Malware. Die größte Gefahr liegt immer noch beim Benutzer (z.B. unvorsichtiges Öffnen von Dateianhängen einer E-Mail). Kennt der Benutzer die grundlegendste Vorgehensweise von Malware, so erhöht sich die Sicherheit des Rechners und Netzwerkes deutlich.

Zentrale Schutzmöglichkeiten

Da der größte Verbreitungsweg von Viren über E-Mails geht, sollte man direkt da ansetzen, nämlich beim Mailserver. Das bedeutet nicht, dass Virens Scanner auf lokalen Rechnern wegfallen dürfen. Virens Scanner, die auf dem Mailserver laufen, nennt man *Mailwalls*. Der Vorteil liegt klar auf der Hand: Sie filtern Viren schon beim Versand aus, so dass diese erst gar nicht mehr auf den Client gelangen. Somit dienen sie als *zentraler Schutz*, der leicht aktualisiert werden kann.

Ein Nachteil ist allerdings die *hohe Serverauslastung*, da jede E-Mail geprüft werden muss und bei großen Unternehmen eine Vielzahl von E-Mails täglich den Mailserver passieren. Der Vorteil überwiegt aber deutlich.

Für einen Aufpreis ist die Mailwall auch schon bei einigen Webhosting-Providern zu haben und es ist nur eine Frage der Zeit, bis sie dem Standard entspricht.

Mail-Provider wie z.B. „GMX“ bieten seit einiger Zeit einen kompletten Virenschutz an, der alle eingehenden und ausgehenden E-Mails, sowie deren Dateianhänge, auf Viren überprüft und aussortiert.

Damit sind zwar Viren, die sich über E-Mail verbreiten unschädlich gemacht, allerdings gibt es auch noch andere Verbreitungswege. Um den Schaden möglichst gering zu halten, sollten Virens Scanner und Firewall am Rande eines Netzwerkes zum Internet aktiv sein. So wird ein mögliches Eindringen der Viren noch vor Eintritt ins Netzwerk verhindert. Es entstehen weniger Kosten und die Sicherheit wird, für alle Arten von Verbindungen die über das Internet stattfinden, erhöht. Die Firewall dient zeitgleich auch als Endpunkt zum Aufbau einer VPN Verbindung.

Für große Firmennetzwerke gibt es Software, mit denen sich ein Administrator kompletten *Überblick über alle Sicherheitsanwendungen* im Netzwerk verschaffen kann. Er kann so, via Fernzugriff von einem Computer aus, alle Anwendungen konfigurieren und aktualisieren. Dies ist viel zeitsparender und nicht mit großem Aufwand verbunden. Der Administrator kann somit das ganze Netzwerk effizient überwachen (beispielhafte Programme wären hier: F-Secure Policy Manager, Symantec Event Manager für Antivirus).

Ein spezielles Anti-Viren-Programm für Datei-Server verhindert, dass Viren keine Chance haben sich weiter im Netzwerk zu verbreiten.

Lokaler Schutz

Eine Statistik von Heise Online beschreibt wie häufig Aktualisierungen durch den Benutzer für Anti-Virensoftware durchgeführt wurden. 26% gaben an, ihre Anti-Viren-Software wöchentlich zu aktualisieren, weitere 43% der Benutzer aktualisieren alle 4 Wochen. Etwa 30% der Befragten aktualisieren ihre Software nicht einmal innerhalb von 4 Wochen. 70% gaben an, Anti-Viren-Software einzusetzen. Man sollte bedenken, dass diese Befragung hauptsächlich von Heise Lesern durchgeführt wurde.

Sicherheitsvorkehrungen

Folgende Sicherheitsvorkehrungen sollten beachtet werden:

- Dateianhänge unbekannter Absender sollten mit Vorsicht behandelt werden. Es handelt sich in vielen Fällen bei den Attachments um Malware.
- Es kursieren heutzutage etliche Falschmeldungen über gefährliche Viren, die jmd. dazu verleiten soll, sich mit falschen Sicherheitsupdates zu schützen. Die Gefahr solcher sog. Hoaxes ist durch die falsch deklarierten Sicherheitsupdates gegeben. Trojaner sind hier nicht selten Bestandteil der Updates. Des Weiteren wird man aufgefordert, möglichst viele über diese Meldung zu informieren → Mail-Server werden unnötig belastet.
- Durch vermehrte Meldungen von Sicherheitslücken in dem Internet Browser der Firma Microsoft, sollte man auf alternative Möglichkeiten ausweichen.
- Neuste Updates für Betriebssystem und Anwendungen installieren (Bsp.: SP2)
- Anti-Viren-Programme sollten die Funktion des LiveUpdates aktiviert haben (Virendefinitionslisten täglich aktualisieren).
- Regelmäßige Backups von wichtigen Daten erstellen.
- Aktuelle Sicherheitssoftware einsetzen (wie Anti-Viren-Programm) kostenlose Software für den privaten Gebrauch: www.free-av.de (Personal Edition), www.ewido.de
- Firewall oder Intrusion Detection System (IDS) einsetzen (bspw. www.zonealarm.de)
- Regelmäßig aktuelle Sicherheitsmeldungen einholen.
- Verwenden Sie möglichst unterschiedliche und sichere Kennwörter (Buchstaben-, Zahlen- und Sonderzeichen-Kombinationen)
- Vorsicht bei Programmen aus unbekanntem Quellen (Tauschbörsen).

6. Bekannte & aktuelle Meldungen aus dem Malware-Bereich

Am 05. Dezember 2004 fand in Amerika eine Konferenz zum Terrorismus statt. Ex-CIA-Direktor Robert Gates sprach davon, dass Computerterrorismus der Wirtschaft erheblichen Schaden zufügen kann.

Bekanntere Beispiele seien hier sicherlich der „Love-Letter“ und ein Test bei dem Spezialisten innerhalb von nur zwei Tagen es schafften, sich Kontrolle über die Stromversorgung einer Stadt zu verschaffen.

Persönliche Erfahrung im IT-Bereich

Vorletzten Sommer (2003) habe ich in einem großen Gelsenkirchener Informatik-Unternehmen ein dreimonatiges Fachpraktikum absolviert. Das Unternehmen entspricht weltweit mitunter den höchsten Qualitäts- und Sicherheitsnormen, verglichen mit anderen Unternehmen der Branche. Das Unternehmen obliegt dem sog. BS-7799-2, wobei nur 5 Unternehmen in Deutschland diesen Qualitätsansprüchen entsprechen.

Nachdem eines Dienstagabends bei mir das Telefon klingelte und ein Freund meinte, dass sein Rechner die ganze Zeit neustarten würde, gab ich ihm einen Tipp das Neustarten zu verhindern. Allerdings war die Ursache nicht gefunden. Ich dachte, es handle sich mal wieder um ein typisches Windows-Problem. Doch nach dem Telefonat kamen weitere Anrufe mit gleichen Problemen. Der Gedanke, dass sich dahinter Malware verbarg, bestätigte sich. Nach Recherchen im Internet konnte ich, aufgrund der Symptome, den Schädling identifizieren.

Am nächsten Morgen bei der Arbeit erfuhr ich, dass sämtliche Rechner alle 5min neustarteten. Damit hatte ich wirklich nicht gerechnet. Der Wurm hatte es geschafft ins firmeninterne Netzwerk einzudringen und verbreitete sich rasend schnell.

Die Telefonanlage der knapp 700 Mitarbeiter wurde von einem VoiceOverIP-Telefonserver im Intranet gesteuert → die Folge: alle Telefongeräte starteten neu. Fast die gesamte Kommunikation im Unternehmen war zusammen gebrochen.

Aufgrund dessen, das ich mich schon am Vortag mit der Problematik auseinander gesetzt hatte, wusste ich, wie man wenigstens die Prozedur des Neustartens verhindern konnte. Doch wer hätte schon einen Praktikanten an die VoiceOverIP-Telefonanlage gelassen? – Mitarbeiter stutzten als ich Ihnen zeigte wie man das Neustarten Ihrer Rechner verhindern konnte – Doch aufgrund dessen, dass gesamte Netze zusammengebrochen waren, konnte nicht wie üblich weitergearbeitet werden.

Dauernd hörte man jmd. fluchen, sah Leute auf dem Flur hin und her rennen die zwecks der internen Kommunikation im Unternehmen die Beine benutzen mussten und viele andere die auf die Kommunikationsvariante der Mobiltelefone zurückgriffen. Ein absolutes Chaos herrschte. Alles nur wegen des Wurms.

Auf die Frage, wo alle hin seien bekam ich die Antwort: „Nach Hause, was sollen die hier noch?“. Ich wunderte mich, wie hilflos ein Unternehmen dieser Branche dem Problem so ausgeliefert war und es nicht mal „eben“ lösen konnte. Maßgeblich war die Aggressivität des Wurms. Kaum ein Unternehmen hätte dies in so kurzer Zeit beheben können.

Man konnte durch die Abteilungen gehen – vorausgesetzt man hatte eine Berechtigung für die Sicherheitstüren, wobei dieses System meines Wissens nach nicht zusammengebrochen war – und sah nur leere Büros. Die gesamte Belegschaft war inzwischen nach Hause gegangen; nun war es auch Zeit für einen Praktikanten wie mich, den Arbeitstag woanders als im Unternehmen ausklingen zu lassen.

Würmer-Infizierung über Sicherheitslücke

Details zum Wurm: W32.Blaster

Der Wurm erreichte weltweit eine Verbreitung wie dies bisher keinem anderen Wurm gelang. Die Infizierung erfolgte rasend schnell, da viele Rechner Sicherheitslücken im System vorzeitig nicht geschlossen hatten, obwohl Microsoft im Vorfeld Sicherheitspatches zur Verfügung gestellt hatte. Der Wurm verbreitete sich insbesondere bei Privatanwendern die in der Vergangenheit über Sicherheitsmechanismen wie Firewalls, nur selten verfügten. Geprägt von weiteren Wurmvarianten in der Geschichte war der W32.Blaster sicherlich ein besonders lauter Alarmton den diesmal auch Microsoft zu hören vermochte. Das ServicePack2 aus dem Hause Microsoft schließt eine Vielzahl von sicherheitskritischen Lücken im Betriebssystem und integriert zugleich ein Sicherheitscenter-Modul in dem, neben einer eingebauten Firewall und einer automatischen Windows-Update Funktion, ein Anti-Viren-Check mit implementiert wurde.

Nun zu den Funktionen des W32.Blasters:

Name:	W32.Blaster
Alias:	W32/Lovsan.worm, W32.Blaster.Worm, WORM_MSBLAST.A
Entdeckt am:	11.08.2003
Verbreitungsweg:	nicht via E-Mail sondern direkt über Netzwerk, da er eine Sicherheitslücke ausnutzt

Der Wurm nutzt einen Fehler in der so genannten *DCOM RPC (Remote-Process-Control)* Umgebung aus. Betroffene Betriebssysteme sind: Windows NT4, Windows 2000, Windows XP und Windows 2003. Bei Windows 95, 98 und ME ist RPC: 135 standardmäßig nicht installiert, sodass der Schädling hier keinen Schaden anrichten kann. Wenn der Wurm ein Opfer im Netzwerk gefunden hat, kopiert er sich nach einem Verbindungsstart über Port 4444 via TFTP:69 (wobei er die „tftp.exe“ aus dem Windows Ordner benutzt) in den Windows Systemordner mit Namen „msblast.exe“ und wartet auf weitere Anweisungen.

Wie die meisten Würmer kopiert sich auch dieser Wurm in die Registrierung unter: HKEY_LOCAL_MACHINE mit Eintrag:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run

Selbst wenn die Infektion nicht erfolgreich verläuft, können Probleme mit der „svchost.exe“ entstehen; auch hier ist ein Download des Microsoft-Sicherheitspatches MS03-26 erforderlich.

Das Ziel des Wurmes ist, Microsoft auf seine unsichere Software hinzuweisen. Am 16.08.2003 startete ein sog. *Distributed Denial-of-Service* Angriff auf den Windows-Update-Server mit der Meldung "*Billy Gates why do you make this possible? Stop making money and fix your software!!*".

Doch waren vorerst nicht nur Microsoft-Produkte dem Wurm hilflos ausgeliefert, sondern auch jene Systeme die ein plattform-spezifisches *Distributed Computing Environment (DCE)* installiert hatten. DCE ermöglicht mit Zuhilfenahme von RPC eine Kommunikation in heterogene Netze – und dies auch über Port 135. DCE ist hauptverantwortlich für das Ressourcen-Management, welches der Blaster nach erfolgreicher Infizierung bei folgenden Betriebssystemen ebenfalls zum Absturz bringt: AIS, Solaris, Linux, Tru64.

Details zum Wurm: W32.Sasser

Name:	W32.Sasser.Worm
Alias:	W32/Sasser.worm [McAfee]
Entdeckt am:	30.04.2004
Verbreitungsweg:	nicht via E-Mail sondern direkt über Netzwerk, da er eine Sicherheitslücke ausnutzt
Art:	Wurm
Größe des Wurms:	15.872 Bytes
Betriebssysteme:	Windows XP, Windows 2000 nicht betroffen: Windows 98/Me/NT
Verbreitung / Risiko	Hoch / mittel
Schadensfunktion	Systemabstürze, verminderte Systemleistung

Sasser existiert in mehreren Varianten die sich aber in ihrer Funktion nicht wesentlich unterscheiden. Alle nutzen die Schwachstelle im sog. Local Security Authority Subsystem Service (LSASS), wovon man auch den Namen ableiten kann. Durch einen „Buffer Overflow“, zu Deutsch Pufferüberlauf, ist es einem Angreifer möglich beliebigen Programmcode auf dem betroffenen System auszuführen und somit volle Kontrolle über den Computer zu erlangen.

Auch wie beim Blaster bedarf es keiner Aktion des Anwenders für die Infizierung. Lediglich eine Verbindung mit dem Internet reicht aus, um potentiell Opfer des Wurms zu werden. Auch hier kommt es zu einer Fehlermeldung, ähnlich dem Blaster, in dem das System binnen einer Minute, wobei ein Abbruch auf normalem Wege nicht möglich ist, herunterfährt. Auch wiederum parallel zum Blaster benutzt der Sasser die FTP-Engine von Microsoft und lädt eine Datei namens „avserve.exe“ in den Windows-System-Ordner und legt einen entsprechenden Registry-Eintrag für das Ausführen des Wurms bei Neustart an. Zudem wird eine Kopie des Prozesses mit Reg.-Schlüssel erzeugt bei dem die ersten 5 Zeichen via Zufall gewählt werden. Sobald die Datei erfolgreich übertragen wurde, wird sie ausgeführt und startet direkt 128 gleichzeitige Angriffsversuche im LAN und WAN.

Würmer-Infizierung via E-Mail

Details zum Wurm: W32.Mydoom

Name:	W32.Mydoom
Alias:	W32/Mydoom@MM, W32.Novarg.A@mm, Shimg, Novarg.A, Mimapil.R
Entdeckt am:	26.01.2004
Verbreitungsweg:	E-Mail
Art:	Wurm
Größe des Anhangs:	22.528 Bytes
Absender, Betreff und Nachricht:	unterschiedlich
Dateiname:	unterschiedlich
Dateiendung:	BAT, CMD, EXE, PIF, SCR oder ZIP
Betriebssysteme:	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
Verbreitung / Risiko	hoch / mittel
Schadensfunktion	Verschickt sich per E-Mail, öffnet Ports, startet DoS Attacke „gegen www.sco.com“

Mydoom trägt einige Einträge in die Registry ein, wodurch der Prozess „taskmon.exe“ bei jedem Systemstart geladen wird (Ähnlichkeit zum Systemprozess „taskmon.exe“).

Er sucht sich Adressen aus bestimmten Dateien von der Festplatte und verschickt sich per E-Mail weiter. Dabei benutzt er nicht alle E-Mail-Adressen, sondern filtert vorher einige aus (falls der Benutzername z.B. die Worte: contact, help, info und webmaster enthält).

Zusätzlich legt er eine „dll“-Datei auf der Festplatte ab, welche einen Backdoor-Trojaner repräsentiert und durch einen Registry-Eintrag bei jedem Systemstart mitgeladen wird. Der *Backdoor-Trojaner* öffnet die Ports 3127 - 3198, mit dem Hacker die Möglichkeit haben sich von außen zu verbinden.

In der Zeit vom 01.02. - 12.02.2004 startete er eine *Denial-of-Service (DoS-) Attacke* gegen die Domain „www.sco.com“ (SCO Group liefert Softwarelösungen für Linux) (DoS: Der Server wird mit unzähligen Anfragen bombardiert und in die Knie gezwungen)

Seit dem 12.02.2004 verbreitet sich der Wurm nicht weiter, allerdings bleibt der *Backdoor-Trojaner* aktiv und ermöglicht weiterhin Fernzugriff.

Details zum Wurm: W32.Bagle

Name:	W32.Bagle
Alias:	W32/Bagle.bd, W32.Beagle.AW@mm, W32/Bagle-AV, I-Worm.Bagle.au, Worm/Bagle.AU, WORM_BAGLE.AU
Entdeckt am:	29.10.2004
Verbreitungsweg:	E-Mail, Peer to Peer
Art:	Wurm
Größe des Anhangs:	19- 28 KB
Absender:	unterschiedlich
Betreff:	Re:, Re: Hello, Re: Hi, Re: Thank you!, Re: Thanks :)"
Nachricht:	:), :))
Dateiname:	Joke, Price, price
Dateiendung:	com, cpl, exe, scr com: ausführbare Systemdatei (command) cpl: control panel extension (Systemsteuerung, Windows) exe: executable file (Dos oder Windows Datei) scr: Screensaver (Systemdatei)
Betriebssysteme:	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
Verbreitung / Risiko	hoch
Schadensfunktion	deaktiviert Sicherheitssoftware und die Internetverbindungs freigabe

W32.Bagle trägt sich in Registry im Schlüssel
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

ein und erstellt Dateien („wingo.exe“, „wingo.exeopen“, „wingo.exeopenopen“) im Windows-Systemverzeichnis.

Schaden: Deaktiviert Virenschanner und Firewall, sowie Internetverbindungs freigabe und Sicherheitscenter von Windows XP mit dem Service Pack 2

Details zum Wurm: W32.Sober Variante Sober.I

Name:	W32.Sober.I Variante vom Sober.H
Alias:	WORM_SOBER.I, W32.Sober.I@mm, W32/Sober.I, Sober.J
Entdeckt am:	19.11.2004
Verbreitungsweg:	E-Mail
Art:	Wurm
Größe des Anhangs:	56.808 Bytes, 46.056 Bytes
Absender:	unterschiedlich
Betreff:	unterschiedlich, täuscht einen Fehler beim Mailprovider vor
Nachricht:	unterschiedlich, unterscheidet zwischen englischen und deutschen Mailadressen
Dateiname:	unterschiedlich
Dateiendung:	unterschiedlich, kann aus zwei Endungen bestehen z.B. name.txt.com
Betriebssysteme:	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
Verbreitung / Risiko	hoch
Schadensfunktion	Versand von Massenmails

Der Wurm Sober.I ist eine in Microsoft Visual Basic geschriebene Variante des Wurmes Sober.H und ist mit UPX gepackt (UPX ist ein Laufzeitpacker, bei Starten des Programms entpackt es sich in den Arbeitsspeicher und wird ausgeführt, kein programmtechnischer Unterschied zu einer normalen ausführbaren Datei). Er erstellt in den Windowssystemverzeichnissen Dateien, die einen aus mehreren Worten zufällig generierten Namen haben. Es werden mehrere Einträge in der Registry vorgenommen (Ausführung des Wurms bei Systemstart). Ist der Wurm aktiv, durchsucht er Dateien mit einer bestimmten Endung (.php, .htm, .ppt und viele weitere) nach Adressen, um sich an diese weiter zu verschicken. Am 16.11.2004 trat der Wurm in Kraft, startete aber erst drei Tage später seine weitere Verbreitung via E-Mail. Das Versenden der E-Mails findet über seine eigens mitgeführte SMTP Engine statt. Vorher überprüft er, ob eine Verbindung zum Internet besteht, indem er über Port 37 und das Network Time Protocol (NTP) versucht einen Server zu kontaktieren. Eine weitere Methode ist die DNS Anfrage an eine Domäne wie bspw. „www.microsoft.com“.

Der Wurm ist in der Lage verschiedene Anti-Viren-Programme zu deaktivieren. Seine Schadroutine ist das Versenden von Massenmails. Die Autoren des Wurms sind weiterhin unbekannt. Es deutet aber einiges auf einen rechtsradikalen Hintergrund hin. Bei älteren Varianten wurden rechtsradikale Nachrichten verbreitet.

7. Zukunftsperspektiven

Gegenwart

Laut einer US-IT-Sicherheitsforschungsgruppe seien Rechner, die nicht mit den neuesten Updates versorgt sind und keine Firewall im Einsatz haben, innerhalb von 20 Minuten im Internet mit Viren oder Würmern infiziert. Zudem sei nun fast jeder PC-Anwender bereits mit Sicherheitsproblemen, Viren und Würmern konfrontiert gewesen und sollte sein System per „Betriebssystem-Update“, Firewall und Virenschanner schützen.

Aufgrund der homogenen Softwarelandschaft von Microsoft, verbreitet sich Malware wesentlich effizienter als früher, wo noch unternehmensspezifische Betriebssysteme liefen, da die meisten Unternehmen standardisierte Software im Einsatz haben. Microsoft ist durch die leichte Bedienbarkeit seiner Produkte von vielen Computer-Benutzern, vor allem Anfängern, bekannt geworden. Dies ging aber nur zu Kosten der

Sicherheit einher, so dass Microsoft auch für seine zahlreichen Sicherheitslücken bekannt ist.

Zudem ist die Kommunikationsdichte enorm gewachsen.

- 234 Mio. Host von etwa 1.2 Mrd. PCs weltweit

Viren und Spam: Bedrohung in E-Mails

Trotz vieler softwarebasierter Lösungen zum Schutz vor Malware in E-Mails, kann nicht garantiert werden, dass aggressive E-Mail Attacken doch zum Endbenutzer durchdringen; auch ist nicht gewährleistet dass alle vertraulichen und unternehmenswichtigen Informationen (wie Angebotsnachfragen) wirklich ankommen und nicht durch ein Filtersystem im Jenseits verschwinden. Noch ist E-Mail weltweit gesehen die wichtigste Unternehmensanwendung schlechthin; doch laut einer Studie würde die Vielzahl der Unternehmer auf eine Nachrichtenaustausch-Alternative ausweichen, um Bedrohungen wie Phishing, Spam oder Malware konsequent auszuweichen.

Virenbedrohung allgemein

Laut einer Umfrage von MessageLabs erwarten mehr als 70% der europäischen Unternehmen in den kommenden zehn Jahren eine Verdopplung der Virenangriffe. Dies ist leider keineswegs Utopie und lässt sich an den folgenden Fakten verdeutlichen:

Die Zahl der Viren steigt und steigt. "Das Verhältnis zwischen Viren und E-Mails lag im vergangenen Monat bei 1 zu 10,7, vor einem Jahr bei 1 zu 125,5 und 2002 insgesamt bei 1 zu 212 - wir haben in die Zukunft geblickt, und sie sieht düster aus" so der Technik-Chef von MessageLabs.

Potentielle Bedrohungen durch Mobilität in den Griff bekommen

Immer mobiler, Erreichbarkeit an jedem Ort der Welt – das ist Zukunft.

In der Zukunft muss es möglich sein, dass Technologien für Notebooks, PDA's und weitere mobile Geräte eingesetzt werden, welche Sicherheitsstellungen der Geräte je nach Umgebung passend einstellen. So sollen sich clientseitige Firewalls bei Integration in einem Firmennetzwerk anders einstellen als bei einer direkten DSL-Verbindung ins Internet. Auch wenn die Software ein Update erfordert, reagiert das moderne System in naher Zukunft dynamisch. Durch so genannte Client-Inspection-Tools wird vor der Netzwerkverbindung nach Viren und Würmern gesucht, um die Konsistenz sicherer Netzwerke weiter auszubauen.

Initiativen wie das von Cisco entwickelte Self-Defending Network gehen hier in die richtige Richtung. Gerade hierbei liegen Strategien zugrunde die es erlauben, das Netzwerk zentral zu adjustieren, d.h. die Clients (wie bspw. ein Notebook, welches Zugang über WLAN erbittet) zu überprüfen und dann in entsprechende Kategorien einzuordnen. Auch die Maßnahme von Live-Sicherheitsupdates wird hierbei automatisiert.

"Code-Check-Tools" – Das Ende der Sicherheitslücken und Buffer Overflows?

Diese Tools prüfen Sequenzen der SourceCodes auf mögliche Inkonsistenzen bzw. Sicherheitsrisiken und markieren potentielle Angriffsflächen des Codes um hier schon bei der Erstellung von Software vorzubeugen. Die meisten Sicherheitslücken beruhen auf „Buffer Overflows“, die sich bekannte Würmer wie der MS Blaster oder Sasser zu Nutze machen.

Gerade weil „Buffer Overflows“ zurzeit noch ein großes Problem bei der Softwareerstellung darstellen, und die großen Hersteller die Problematik auch insbesondere bei Drittherstellern befürchten, möchten diese bereits bei den Entwicklungstools für mehr Sicherheit sorgen. So bietet Microsoft erstmals

registrierten Entwicklern an, diese bei dem Umgang der Speicherverwaltung durch Online-Dokumentationen zu schulen. Doch Microsoft geht noch einen Schritt weiter und bietet des Weiteren Online-Trainings zu den geplanten Updates an.

Experten befürchten, dass durch die Benutzung solch innovativer Tools die Softwarehersteller in naher Zukunft die juristische Verantwortung für die Folgen von Sicherheitslöchern übernehmen müssten.

Künftig würden Unternehmen den Einsatz von unsicherer Software nicht mehr akzeptieren. Sicherheit werde mehr und mehr zur Grundvoraussetzung behaupten die Hersteller solcher Code-Checking-Tools. Und dies ist sicherlich kein Wunschgedanke der Hersteller. Existieren erstmal qualitativ gute Programme, die die o.g. Mechanismen zur Ausmerzung der Sicherheitslücken an richtiger Stelle einsetzen, wird sich unserer Meinung nach bestimmt ein fundamentaler Wandel vollziehen.

Schlusswort

Um Virenautoren schneller ausfindig zu machen, hat Microsoft für jeden Hinweis, der zum Autor eines gefährlichen Wurmes führt, eine Belohnung in Höhe von \$250.000 ausgeschrieben.

Zitat vom Pressesprecher Alex Günsche der Protect Privacy Organisation: „Die Wahrheit liegt, wie so oft, irgendwo in der Mitte. Ein Ende der Viren-, Würmer- und Spam-Seuche ist genau so illusorisch wie der ewige Weltfrieden.“

Es ist vorausschaubar, dass sich in Zukunft an der schnellen Verbreitung von Viren, Würmern und Trojanern nichts ändern wird. Im Gegenteil, es werden sogar noch mehr Schädlinge unterwegs sein, als je zuvor. Der Einsatz von Sicherheitssoftware wie eine Firewall und ein Virens Scanner sind schon heute unabdingbar. Sollte sich nichts an den Tatsachen ändern, so wird sich der Trend weiter fortsetzen. Wir brauchen ein System, dass in Echtzeit Viren erkennt und unschädlich macht. Das Ganze darf nicht nur lokal passieren, sondern muss zentral für ein ganzes Netzwerk greifen.

8. Gespräch mit Sophos (Christoph Hardy | PR / Communication Coordinator)

Wie viele Viren (gesamte Malware) werden derzeit mit Ihrem Programm erkannt?

Sophos AV schützt derzeit vor 97622 Viren, Würmern und Trojanern.

Die Sophos-Software wird derzeit auf 28 unterschiedlichen Betriebssystemen unterstützt.

(Stand 30.11.2004, 12:00); Tendenz: steigend.

Jeden Monat kommen ca. 300 - 400 'neue' dazu.

Einen statistischen Überblick der monatlichen 'Top Ten' unter:

<http://www.sophos.de/virusinfo/topten/>

Schadprogramme unter Linux/Unix: ca. 150 - 200

Macintosh: ca. 55

Rest: Microsoft Windows

Wie lange dauert heutzutage das Verfahren zur Erzeugung einer Anti-Virenroutine bzw. die Erstellung eines Removal-Tools?

Das hängt von der Komplexität der Malware ab. Durchschnittlich entstehen Anti-Viren-Routinen zwischen 30 Minuten und zwei Stunden.

Bei Removal-Tools ist dies ähnlich. Wird ein Removal Tool neu erzeugt dauert dies etwas länger, da für die Entfernung der Viren-Sideeffekt berücksichtigt werden muss. Sämtliche Windows Sprachversionen müssen beachtet werden (z.B. in der Registry).

Wie gut sind Heuristikverfahren?

Sophos setzt eher auf die sog. Sequence-Technology bzw. proaktive Erkennung von Viren.

Die Sequence-Technologie ist eine neue Methode, mit der komplette Wurm-Familien zuverlässig erkannt werden können. Der große Vorteil der Sequence-Technologie ist, dass neue Varianten eines Wurms proaktiv erkannt werden. Das heißt im Klartext: Es muss keine neue IDE für eine Variante entwickelt werden, um sie unschädlich machen zu können. Die neue Sequence-Technologie bringt also ein enormes Sicherheits-Plus. Denn damit werden zukünftige Wurm-Varianten von Anfang an abgeblockt.

Die Methode ist sicherer als Heuristik.

Obwohl unbekannte Varianten eines Wurms mit der Sequence-Technologie erkannt werden, ist das neue Feature keine heuristische Methode. Denn es wird weiterhin eine Virenkennung entwickelt, die für die Erkennung der ersten Variante eines Wurms nötig ist.

In der Virenkennung „W32/Beispielwurm-Gen“ ist die Code-Struktur für die Erkennung eines bestimmten Wurms festgelegt. Sobald Sophos Anti-Virus ein Schadprogramm entdeckt, das zu einem gewissen Prozentsatz dieser Struktur entspricht, schließt es auf eine Variante dieses Wurms.

Die zuverlässige Erkennung wird dadurch möglich, dass der Code in bestimmte Einheiten (Sequences) eingeteilt wird, die zusätzlich anhand ihrer Bedeutung innerhalb des Programm-Codes gewichtet werden.

Die neue Technologie ist derzeit auf alle „C++“-Würmer und Trojaner anwendbar – also auf die Mehrheit der aktuell bekannten Würmer. In Zukunft soll sie nicht nur auf die Erkennung von Viren ausgedehnt werden – sondern auch auf Schadprogramme, die in der Programmier-Sprache „Delphi“ geschrieben wurden.

Wie viele Viren, Würmer und Trojaner-Neuerscheinungen haben Sie in etwa pro Tag?

sehr unterschiedlich, zwischen 1 und 15, durchschnittlich aber 3 bis 4.

Was war Ihr größter Anti-Viren Erfolg?

Jeder erfolgreich bekämpfte Virus ist ein Erfolg!

Beispiel könnten aber sein Bugbear-A oder Blaster-A, für die Sophos sehr schnell Virenkennungen für Kunden zur Verfügung gestellt hat.

10. Literatur und Quellenangabe

Bücherangaben

Dr. Klotz' Computerschutz

Dr. Karlhorst Klotz

Verlag: mitp

Das Anti-Viren-Buch

David Harley, Robert Slade, Urs E. Gattiker

Verlag: mitp

hacker's guide - Sicherheit im Internet und im lokalen Netz

Anonymous

Verlag: Markt & Technik

Anti-Hacker Buch

Online-Referenzen

<http://www.bul-online.de>

<http://www.theparallax.org>

<http://www.antivirus-online.de>

<http://www.poose.de>

<http://www.kreideholen.de>

<http://www.trojaner-info.de>

<http://www.emsisoft.de/de>

<http://www.golem.de>

<http://www.heise.de>

<http://online.securityfocus.com>

<http://www.antivir.de>

<http://www.symantec.de>

<http://www.trendmicro.com>

<http://www.bsi.bund.de>

<http://www.virus-informer.de>

http://agn-www.informatik.uni-hamburg.de/agn_avlinks.htm

<http://www.virus-aktuell.de>

<http://www.virusbtn.com>

<http://www.cisco.com>

Sonstiges

Sicherheitstest:

<http://security.symantec.com/sscv6/default.asp?productid=symhome&langid=ge&venid=sym>

Flashanimation zur Geschwindigkeit und örtlichen Verbreitung von bestimmten Würmern

<http://www.pandasoftware.com>

zum Programm Stinger

<http://vil.nai.com/vil/stinger/>

Virens Scanner Test der Zeitschrift Chip Mai 2004

http://www.chip.de/artikel/c_artikel_11796074.html

Ein Projekt der Arbeitsgruppe Wirtschaftsinformatik am Institut für Technische und Betriebliche Informationssysteme der Otto-von-Guericke-Universität Magdeburg in Zusammenarbeit mit der AV-Test GmbH.

Führen Tests für die Hersteller der Anti-Virensoftware und für Zeitschriften durch.

<http://www.av-test.org/>

Viren Enzyklopädie

<http://www.avp.ch/avpve>