SEMINAR

INTERNETDIENSTE

SS 2004

Thema:

Viren, Würmer und Trojaner – und ihre wirtschaftlichen Auswirkungen

Prof. Dr. Franz Schweiggert

Abteilung SAI

Bearbeitet von:

Markus Cramer

Inhaltsübersicht

1. Einleitung

„Das Internet ist kein Ort mehr, wo man sicher seinen Geschäften nachgehen kann. Legitime Anwender werden zu Opfern von Spammern, Virenautoren und Hackern. Ohne einen aktuellen Schutz gefährdet Cyberkriminalität jeden von uns“ [1].

Costin Raiu
Leiter Forschung und Entwicklung, Kaspersky Labs Rumänien

Fernsehsender und Zeitungen berichten von den neuesten Viren-Epidemien und selbst Menschen, die niemals einen Computer benutzt haben, ist dies ein vertrauter Begriff.
Es ist aber notwendig zu unterscheiden, denn nicht jeder Schädling fällt unter den Begriff des „Virus“, der sich umgangssprachlich eingebürgert hat und auch nicht jedes Web-Ungeziefer ist per se ein zerstörerisches Programm.

Vom Fachmann als „Malicious Software“ oder kurz „Malware“ bezeichnete böswillige Software kennt neben klassischen Viren noch viele verschiedene andere Arten wie Internet- und eMail-Würmer, Trojaner, Backdoors, Spams, Cookies usw.
Allerdings kann die Trennung nicht immer sauber erfolgen, da die Schädlinge oft mehrere Charakteristika vereinen wie beispielsweise viele eMail-Würmer, die auch Viren-Funktionen aufweisen.

Unbeachtet seiner Gattung ist das Ziel eines Virus-Programms, sich vom Anwender unbemerkt über Rechner und Netzwerke zu verbreiten. Die Auswirkungen („Payloads“) eines solchen Programms können je nach Funktionsweise des Virus sehr unterschiedlich sein. Es ist möglich, daß ein Virus dazu programmiert wurde, lediglich eine humorvolle Nachricht auf dem Monitor abzuspielen, alle Daten auf dem Rechner zu löschen oder eventuell auch, um vertrauliche Daten auszuspionieren und diese zu verbreiten.

Man ist geteilter Meinung, ob die ersten Viren Ende der 60-er oder Anfang der 70-er Jahre des vergangenen Jahrhunderts auftauchten. Es ist aber eindeutig festzustellen, daß ihre Auswirkungen damals äußerst begrenzt und unproblematisch waren, da die Anzahl der Computernutzer um ein vielfaches geringer war als heute. Mit der immer schneller voranschreitenden Entwicklung, nicht nur Unternehmen sondern auch Haushalte mit dem Internet zu verbinden, und der immer stärkeren Verflechtung untereinander wachsen auch beständig die Ausbreitungs- und Schädigungsmöglichkeiten von Viren, Würmern und Consorten. Wenngleich auch Scherzprogramme im Umlauf sind („Hoaxes“), die keinen Schaden anrichten und nur Panik verbreiten, so ist die Bedrohung durch Viren eine alltägliche Erscheinung, mit der nicht zu spaßen ist. Die Häufigkeit der Angriffe und die Geschwindigkeit der Ausbreitung nehmen täglich zu und haben in ihren Folgen horrende Verluste für Unternehmen und Privatanwender von mehreren Milliarden Euro pro Jahr.

2. Viren, Würmer und Trojaner

2.1 Unterscheidung von Viren, Würmern und Trojanern

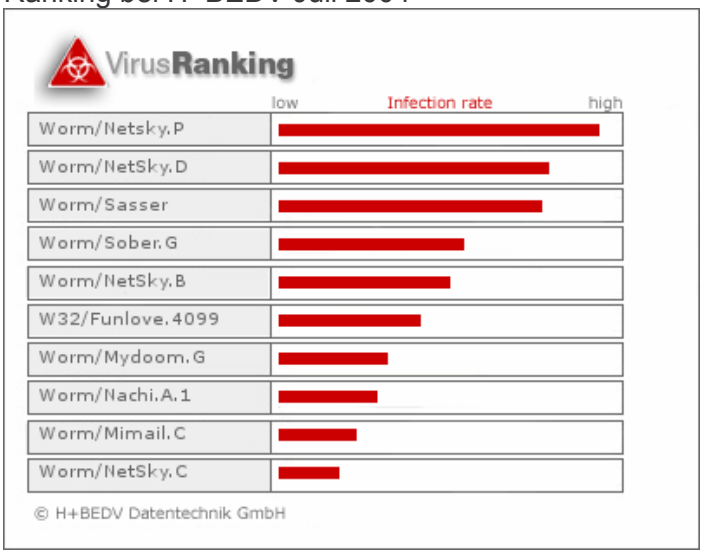
Viren
Ein Virus ist ein Programm, das unbemerkt in den Computer gelangt und sich in die Befehlskette eines anderes Programm einschleust und dieses somit „infiziert“. Beim Versuch, das infizierte Programm auszuführen, wird gleichzeitig oder stattdessen der Virus ausgeführt. Viren vermehren sich und zeigen verscheidenste Arten von Schädigungen:

Würmer
Würmer sind im Prinzip Viren, die sich ohne Wirt selbst weiterverbreiten können. „Es sind eigenständige Programme, die Routinen besitzen, um sich auf andere Rechner zu kopieren“ [2].
Sie kommen über Schnittstellen zwischen Computer und Internet (Ports), am häufigsten aber nutzen sie E-Mail als Verbreitungsweg und verschicken sich hier „als (meist direkt ausführbares) Attachment an mehr oder weniger zufällig ausgewählte Mail-Adressen. SirCam oder Kournikova sind berüchtigte Beispiele dieser Gattung. Für gewöhnlich erfordern Würmer eine Aktion des Anwenders (Ausführen des Attachments), um aktiv zu werden, Nimda nutzte jedoch eine Sicherheitslücke, die ihn automatisch bei Betrachten der Mail in Microsoft Outlook und Outlook Express startete“ [2].

Trojaner
Bei einem trojanischen Pferd oder kurz Trojaner handelt es sich um „Viren und Würmer, die sich in harmlosen Programmen verstecken (€URO 05 /2004, S.24)“. Sie geben vor, etwas Nützliches oder Wünschenswertes zu tun (machen das vielleicht auch wirklich), führen aber gleichzeitig eine bestimmte Aktion aus, die nicht erwartet oder gewünscht war. Dazu zählt in erster Linie die Datenspionage (beispielsweise das Ausspähen von Passwörtern) oder die Zerstörung des Wirtssystems.
„Eine besonders aggressive Form des Trojanischen Pferdes sind so genannte Backdoor-Trojaner. Diese richten auf dem Wirtssystem Ports (Backdoors) ein, durch die ein Hacker einfallen kann. Mit Hilfe von Backdoor-Trojanern kann der Hacker auf fremde Rechner zugreifen und hat dann die Fernkontrolle über praktisch alle Funktionen [3]“. „Ein berüchtigtes Beispiel ist Back Orifice [...]. Dieses Programm nistet sich im Hintergrund eines Windows-Rechners ein und ermöglicht fortan die komplette Kontrolle von außen [4]“.

2.2 Viren-Ranking nach Auftreten und Infektionsrate

Ranking bei H+BEDV Juli 2004 [5]

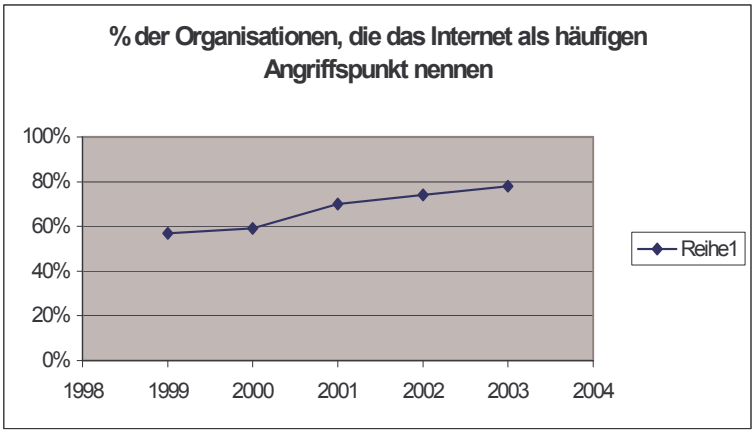


Top 10 für Mai 2004 bei Kaspersky Labs [6]

Position	Veränderung der Position	Name	Auftreten in Prozent
1	5	I-Worm.Netsky.aa	31.47%
2	-1	I-Worm.Netsky.b	30.98%
3	-1	I-Worm.Netsky.q	6.89%
4	5	I-Worm.Netsky.y	5.03%
5	Neu	I-Worm.Bagle.z	5.00%
6	-1	I-Worm.NetSky.d	3.12%
7	7	I-Worm.LovGate.w	1.74%
8	-5	I-Worm.NetSky.t	1.66%
9	1	I-Worm.Swen	1.56%
10	-3	I-Worm.Mydoom.e	1.32%

2.3 Das Internet als Quelle der Bedrohung

Knapp 80 Prozent aller Organisationen benennen das Internet als eine Quelle häufiger Angriffe. Dabei steigt der Prozentsatz seit der letzten Jahre kontinuierlich.



Quelle: (www.astaro.com/data/pdf/whitepapers/Whitepaper_ImprovedNetworkSecurity_en.pdf, 29.06.04)

Aber nicht nur die Zahl der Angriffe steigt, auch die ständigen Variationen und Unterschiede in den Angriffsarten erhöhen das Gefahrenpotential des Internets. Hierbei sind Viren mit über 80 Prozent auf Platz 1 der Angriffsarten.

3. Allgemeine Schäden

3.1 Primäre Schäden

Direkte Auswirkungen eines Virenbefalls [7]
Man kann unterscheiden zwischen absichtlichen Schäden (z.B. Zerstörung oder Korruption von Dateien, Dateispionage), zufälligen Schäden (z.B. Korruption des Systembereichs, was dazu führt, dass das Wirtssystem nicht booten kann) und eher nebensächlichen Schäden, die nicht offensichtlich oder schwerwiegend sind, die jedoch auf die Tatsache der Infektion zurückzuführen sind (z.B. verringerte Speicherkapazität, Festplattenkapazität oder Prozessorzyklen).

Versuche, die Existenz des Virus zu verstecken, kann außerdem zu bewussten oder zufälligen Beschädigungen führen, wenn die Umgebung manipuliert oder neu konfiguriert wird (Beispiele hierfür sind: Verschwinden von Word-Menüoptionen, die mit dem Vorhandensein von Makros zu tun haben, Verschlüsselung oder Verschiebung von Systembereichen beispielsweise vom Master Boot Record, Manipulation der Windows-Registry).

Die Folgen eines Virenbefalls sind je nach Art der Malware sehr unterschiedlich und können von einfachen Bildschirmanimationen bis hin zum totalen Datenverlust reichen.

Beispiele zur Störung des Arbeitsablaufs des Computers [7]
Der Herbstlaubvirus (auch Cascade beziehungsweise 1701-Virus genannt) lässt die Buchstaben auf dem Bildschirm nacheinander nach unten fallen, wo sie sich anhäufen. Bei jedem Auftreffen eines Buchstabens auf den unteren Bildschirmrand ertönt aus dem eingebauten Lautsprecher ein Klicken. Die Bildschirmanzeige wird unlesbar und ein weiteres Arbeiten ist schwer möglich. Startet ein Benutzer den Computer an dieser Stelle neu, so ist jede nicht gesicherte Datei verloren. Im schlimmsten Fall kann somit eine benutzte Datenbank zerstört werden, da die Datenbankdateien nicht ordnungsgemäß geschlossen wurden.

Der MIX-1 Virus stört das Ausdrucken von Texten und Grafiken auf einem Drucker. Er ersetzt dazu mit Hilfe einer Tabelle auszudruckende Buchstaben durch andere Buchstaben: Zum Beispiel wird der Text "Sehr geehrte Damen und Herren" ersetzt durch "Rahr gaahrta Deman ond Harran". In diesem Fall kann der infizierte Computer für Geschäftsbriefe nicht mehr verwendet werden.

Beispiele zur Zerstörung von Daten [7]
Der DATACRIME-II Virus führt bei einer Aktivierung zwischen dem 13. Oktober und dem 31. Dezember jeden Jahres (außer Montags) eine Low-Level-Formatierung der ersten Spuren der Festplatte durch, so dass ein Benutzer auf die Daten der Festplatte nicht mehr zugreifen kann und die Festplatte neu einrichten muss.

Der Michelangelo Virus zerstört jedes Jahr am 6. März, dem Geburtstag des italienischen Bildhauers und Malers Michelangelo Buonarotti, den Datenträger. Dazu werden bei AT und PS/2 Systemen auf den Festplatten die Sektoren 1-17; Kopf 0-3 auf allen Spuren mit unsinnigen Werten überschrieben. Bei Disketten zerstört dieser Computervirus, abhängig vom Format, die Sektoren 1-9 beziehungsweise 1-14.
Die Zerstörung von Daten durch Computerviren kann fatale Folgen haben. Werden zum Beispiel in einem Versicherungsunternehmen sämtliche Kundendaten gelöscht, ist ein weiteres Arbeiten des Versicherungsbetriebes nicht möglich, falls keine Datensicherung vorgenommen wurde.

Ebenfalls kann die Zerstörung von Daten fatale Folgen für Patientendateien in Krankenhäusern haben. Gehen dort Eintragungen über lebenswichtige Medikamente für

bestimmte Patienten verloren, ist eine Versorgung dieser Patienten mit diesen Medikamenten nicht mehr gewährleistet.

3.2 Sekundäre Schäden

Neben den primären, technischen Schäden hat ein Virus, Wurm oder Trojaner auch sekundäre Auswirkungen wie Verunsicherung oder Panikreaktionen der Anwender aber auch ein Vertrauens- und Imageverlust des betroffenen Unternehmens. Das stellt auch den Grund dar, warum betroffene Unternehmen es vermeiden, öffentlich Schwierigkeiten oder gar Schäden durch Malware einzugestehen.

Beispiel T-Online: Schaden durch Sasser, aber keine Klage
Das Beispiel von T-Online bestätigt die Erfahrung, daß von Viren betroffene Großunternehmen nicht sonderlich gewillt sind, diese Schäden öffentlich zu diskutieren. Auch die Entscheidung, keine Klage gegen den Sasser-Autor einzureichen, zeigt deutlich in diese Richtung.
Mitte Mai noch hatte die Pressestelle von Wurm-Befällen nichts wissen wollen, „man sei lediglich indirekt betroffen“[8], hieß es. Erst nachdem Heise Security auf Auszüge des Troubleticket-Systems „Mars“ verwies, die der Redaktion vorlagen, räumte der T-Online Pressesprecher Michael Schlechtriem ein, es habe "bei T-Online im Rahmen des Installationsrollouts des Securitypatches von Microsoft intern einzelne Arbeitsplatzsysteme" gegeben, "die kurzzeitig nicht zur Verfügung standen“ [8].

Das war leicht untertrieben. Die Troubletickets „bestätigen die Hinweise, wonach es bei T-Online zu teilweise massiven Problemen durch Sasser kam. Ein Eintrag zum ‚Virenbefall durch den Internetwurm Sasser‘ dokumentiert das Ausmaß:
Betroffener Service ‚intranet plattform (intern)‘, Wirkbreite ‚national‘, Servicebeschränkung ‚sehr hoch‘, Störungsbeginn ‚3.5.2004‘, Störungsende ‚12.5.2004‘.
Einzelne Tickets sprechen eine beredte Sprache. Ein Mitarbeiter aus Oldenburg beklagt, ‚dass am gesamten Standort offenbar sämtliche Rechner befallen sind und sich selbsttätig herunterfahren‘. Noch am nächsten Tag stellt ein Mitarbeiter in Darmstadt fest, dass es nicht möglich sei, den Patch einzuspielen, da die Intervalle zwischen den Neustarts eindeutig zu kurz seien; ein Service-Mitarbeiter in Darmstadt warnt: ‚Es ist möglich, dass es Netzwerkprobleme aufgrund der derzeitigen Wurmproblematik (Sasser) gibt.‘“ [8].

Weitere Beispiele für sekundäre Schäden
„Banken in den USA und Rußland kappten schon mal für zwei Tage die Geldautomaten. In einem deutschen Katasteramt wurden sechs Monate lang alle Bytes vertauscht, bei einem Autohersteller änderten Viren die Meßwerte beim Produkttest – und im Internet eines namhaften deutschen DAX-Unternehmens tauchten plötzlich die Inhalte der Vorstands-PCs auf“ (€URO 05 /2004, S.24ff).

Einer Umfrage des Wirtschaftsmagazins €URO zufolge hatten mehr als die Hälfte aller Manager bereits Probleme mit Viren, Würmern und Trojanern, mißtrauen ihrem PC und glauben, daß sie ausspioniert werden. (Umfrage im April 2004 im Auftrag von €URO unter 561 Managern und Unternehmern durch empirica@ag, Köln. Veröffentlicht in €URO 05/2004).

Aufgrund der Bedrohung durch Malware scheuen laut Trans Atlantic Consumer Dialogue, einem Forum von US- und EU- Verbraucherverbänden, 52 Prozent aller Internet-User davor zurück, im Internet einzukaufen (€URO 05 /2004, S.24).

4. Wirtschaftliche Schäden

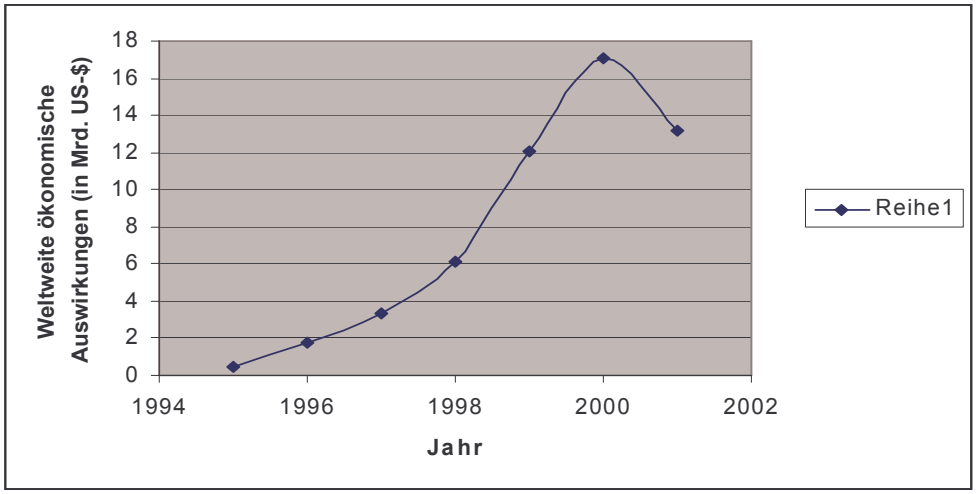
Die zuvor beschriebenen Auswirkungen und Bedrohungen eines Virenbefalls „haben dadurch auch nicht unwesentliche Kosten zur Folge:

- Zeit, Kosten, Personal und Software für die Beseitigung des schädlichen Codes
- Zusätzlich zu ergreifende organisatorische Abwehr-Maßnahmen
- Wiederherstellung zerstörter Daten bzw. Geräte
- Entgangener Umsatz durch Geheimnisverrat und Image- / Vertrauensverlust
- Entgangener Umsatz und verlorene Produktivität durch Systemausfall
- Inkorrekte Datenverarbeitung wegen gefälschter Daten“ [9]

4.1 Weltweiter wirtschaftlicher Schaden von Malware – ein Rückblick

Trend Micro, das japanische Unternehmen für IT-Sicherheit, veröffentlichte 2002 in seinem Whitepaper „The real cost of a virus infection“ [10] die Zahlen einer Umfrage des Computer Security Instituts. Hierbei wurde deutlich, daß 85% aller Antwortenden in den letzten 12 Monaten einen Sicherheitsdurchbruch festgestellt hatten. Die 35 %, die einen wirtschaftlichen Schaden meldeten, bezifferten diesen auf 377.828.700 US-Dollar.

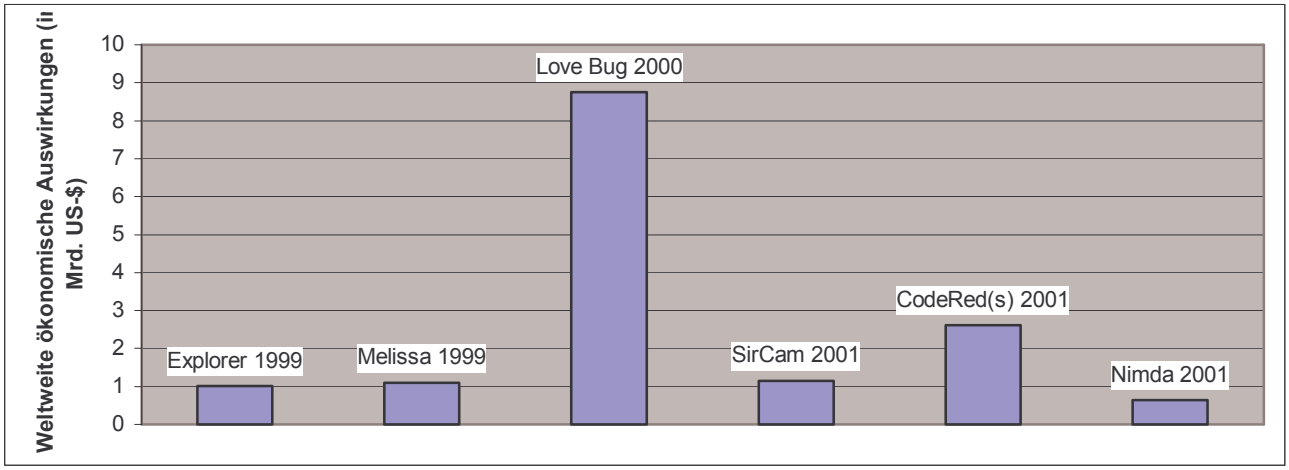
Nach der Analyse von Computer Economics lassen sich für die zurückliegende Jahre folgende Schadenssummen feststellen, die auf Attacken von Malware zurückzuführen sind.



Quelle: Computer Economics 04.01.2002, www.computereconomics.com (24.05.2004)

Der weitere Trend
Ende Februar nach Veröffentlichung dieser Zahlen schätzte die Radicati Group den wirtschaftlichen Schaden von Malware für das laufende Jahr 2002 auf 21 Milliarden US-Dollar und prognostiziert für 2006 einen Wert von 54 Milliarden US-Dollar [11].

Wirtschaftlicher Schaden von speziellen Viren, Würmern und Trojanern
In dem folgenden Diagramm sieht man sehr deutlich die verheerende Auswirkung des „I love You“-Virus und somit auch eine Erklärung für die besonders hohen wirtschaftlichen Schäden im Jahr 2000.



Quelle: Computer Economics 04.01.2002, www.computereconomics.com (24.05.2004)

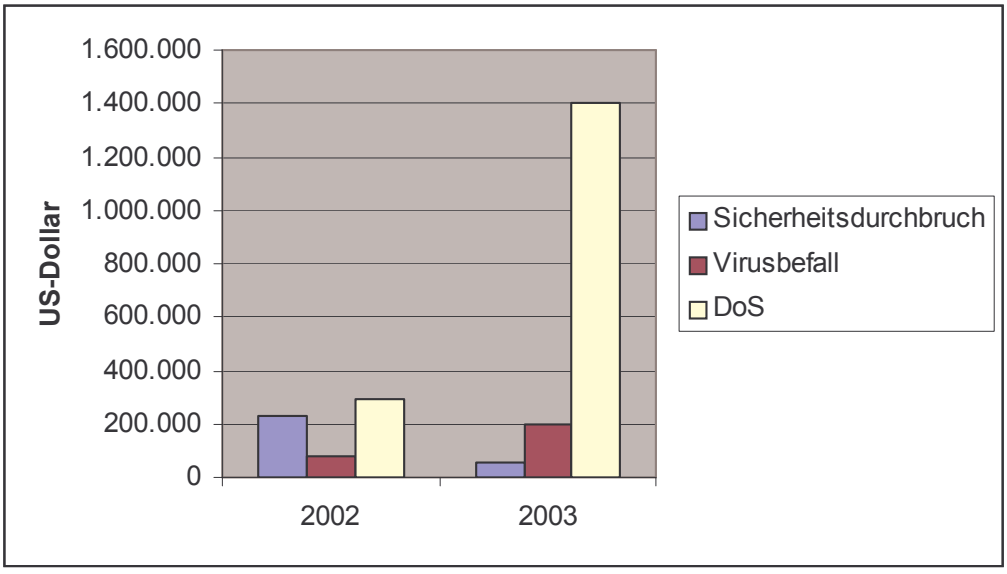
4.2 Weltweiter wirtschaftlicher Schaden durch aktuelle Malware

Kosten für ein deutsches Kleinunternehmen und Europas Wirtschaft
Der Virenbefall eines deutschen Kleinunternehmens kostet im Schnitt 5000 Euro, das ergab eine Studie von Network Associates – „ein Drittel aller Betroffenen mußte neue Hardware anschaffen. Für Europas Wirtschaft beträgt der Schaden 22 Milliarden Euro pro Jahr“ (€URO 05 /2004, S.24).

Durchschnittliche Kosten von Virenbefall, Sicherheitsdurchbruch und DoS-Attacke
Weitere Zahlen veröffentlicht die Astaro AG, ein Unternehmen zur Entwicklung von Lösungen zur IT-Sicherheit, in seinem Whitepaper zu Netzwerksicherheit:

Für das Jahr 2002 entstanden durchschnittliche Kosten von 226.000 US-Dollar für einen Sicherheitsdurchbruch von außen, 81.000 US-Dollar für einen Virusbefall und 297.000 US-Dollar für eine Denial of Service- Attacke [12].

Für das Jahr 2003 entstanden durchschnittliche Kosten von 56.000 US-Dollar für einen Sicherheitsdurchbruch von außen, 200.000 US-Dollar für einen Virusbefall und 1.400.000 US-Dollar für eine Denial of Service- Attacke [13].



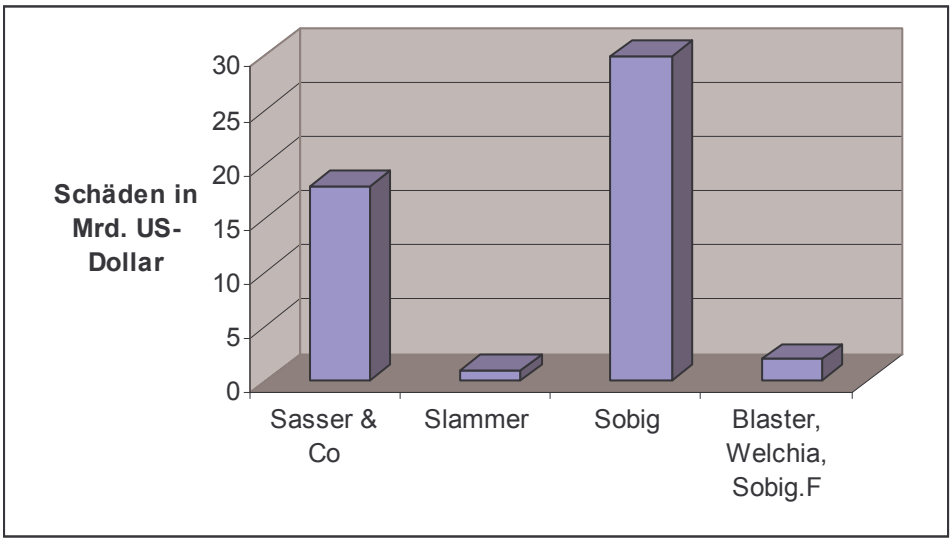
4.3 Die Auswirkungen aktueller Malware an Beispielen

Die Schäden des Sasser-Wurms
Mai 2004 war der fünft-schlimmste Monat, was Attacken von Viren, Würmern und Trojanern betrifft und hat einen geschätzten weltweiten wirtschaftlichen Schaden zwischen 16,2 – 19,8 Milliarden US-Dollar verursacht. Dies ist hauptsächlich auf den Ausbruch des Sasser-Wurms und entsprechender Varianten zurückzuführen [14].

Die Schäden des Slammer-Wurms
Das Unternehmen für Internet-Sicherheit Mi2g schätzt, daß der Slammer-Wurm annähernd eine Milliarde US-Dollar an Aufräumkosten und wirtschaftlichem Schaden verursacht hat. Hierbei berücksichtigt sind auch Einbußen im Verkauf und der Produktivität, die durch Ausfälle des Internets und Systemprobleme verursacht wurden [15].
Die Schäden des Sobig-Virus
Ein im April veröffentlichter Science Artikel spricht allein dem Sobig-Virus wirtschaftliche Schäden von 30 Milliarden Dollar zu [16].

Komplexe Bedrohungen – die Schäden von Blaster, Welchia und Sobig.F
Nach dem Internet Security Threat Report von Symantec waren komplexe Bedrohungen „verantwortlich für einige der bedeutendsten Sicherheitsvorfälle des Jahres. Im August wurde die Internetgemeinschaft in nur 12 Tagen mit drei neuen Würmern der Kategorie 4 (von insgesamt 5 Bedrohungsstufen, wobei 5 die höchste Stufe ist) konfrontiert. Diese Würmer – Blaster, Welchia und Sobig.F – infizierten Millionen von Computern weltweit und sollen, nach Schätzungen von Computer Economics, Schäden von bis zu 2 Milliarden US-Dollar verursacht haben“ [17].

Dies sei zusammenfassend in einer Grafik dargestellt:



5. Ausblick

Stark gestiegene Wahrscheinlichkeit einer katastrophalen Malware-Attacke
„Es ist heute kein Problem mehr, die Internet-Infrastruktur jedes Landes lahm zu legen (€URO 05 /2004, S.27)“, behauptet Christian Ebert, Sicherheitschef der Kölner Telekomfirma QSC. Er erlebte bereits „eine der gefürchteten ‚Denial of Service‘-Attacken, bei denen Hunderttausende von Rechnern per Trojaner aktiviert und konzentrisch auf einen Endanschluß fokussiert werden, um ihn lahm zu legen. Die Belastung stieg dabei stundenlang auf ein Gigabyte pro Sekunde“ (€URO 05 /2004, S.27).

Die Wahrscheinlichkeit einer katastrophalen Malware-Attacke, definiert als weltweite wirtschaftliche Schäden im Ausmaß von 100 Milliarden US-Dollar durch eine Kette kombinierter Ereignisse, ist sprunghaft gestiegen. Lag sie 2003 noch gerade mal bei 2,5 %, so beträgt sie in 2004 mittlerweile alamierende 30 % [14].

Angriffsmethoden zukünftiger Würmer
Amichai Shulman analysiert in seinem Artikel „Web Application Worms: Myth or Reality“ [18] „das Potenzial einer neuen Gattung von Würmern, die gezielt Web-Applikationen angreifen und automatisiert in Systeme eindringen. Dabei setzen sie Techniken ein (War Searching), die sich an die Funktion heutiger Web-Suchmaschinen anlehnen: Mit Schwachstellen-Scannern durchsuchen sie einen Server nach Sicherheitslücken und dringen mit dem passenden Exploit ein. Damit könnten sie weit erfolgreicher als SQL Slammer, Code Red und Blaster sein“ [19].

In ‚Flash Worms: Thirty Seconds to Infect the Internet‘ stellen die Autoren von SiliconDefense fest, „dass es kein Problem sei, vorab eine nahezu komplette Liste aller verwundbaren Systeme zu erstellen. Dazu bräuchte man lediglich eine etwa 48 MByte große Tabelle, die die geschätzten 12 Millionen Web-Server und die darauf laufende Software auflistet. Eine solche Liste ließe sich beispielsweise mit Web-Spiders, wie sie auch Suchmaschinen benutzen, leicht erstellen. Damit könnte dann ein Flash-Wurm in Sekundenschnelle quasi das gesamte Internet infizieren – beziehungsweise den von der gerade aktuellen Sicherheitslücke betroffenen Teil. Man darf wohl getrost davon ausgehen, dass solche Listen bereits existieren oder gerade erstellt werden. Die Chancen, solche Aktivitäten zu entdecken, sind bei vorsichtiger Vorgehensweise äußerst gering“ [20].
Ein solcher Wurm könnte theoretisch in 30 Sekunden das ganze Internet infizieren. Das greift auch ein aktueller Science-Artikel [16] auf. Die Autoren fürchten, daß ein Wurm dieser Art und Geschwindigkeit das ganze Internet lahm legen könnte – oder schlimmer. Es ist offensichtlich, daß die weltweiten wirtschaftlichen Folgen eines solchen Angriffs alles bis jetzt Dagewesene weit übertreffen werden.

Als Gegenmaßnahmen diskutieren die Autoren die Möglichkeiten, „die Ausbreitungsgeschwindigkeit von Viren und Würmern zu bremsen. Der Vorschlag der Autoren lautet: Drosseln (Throttling). Sie stellen fest, dass eine Begrenzung der Zahl der neuen Verbindungen, die ein Computer pro Zeiteinheit aufbauen darf, die Ausbreitungsgeschwindigkeit von Viren drastisch senken könnte, ohne die normale Nutzung des Internets zu beeinträchtigen“ [21].

6. Fazit

Es ist eine erfreuliche und höchst notwendige Entwicklung gewesen, daß die Sensibilisierung in der Bevölkerung für die Bedrohung durch Viren, Würmer und Trojaner in letzter Zeit stark zugenommen hat. Auch die Hilfen, dieser Bedrohung entgegenzutreten, wurden deutlich verbessert. Wie es in der Medizin eine ernsthafte Forschung gibt, zu jedem auftretenden Virus das Gegenmittel zu finden, so gibt es auch im Bereich der IT-Sicherheit Spezialisten, die Virenprogrammierern Paroli bieten. So stehen Privatanwendern mittlerweile freie Antiviren-Programme und Firewalls zum Schutz der heimischen PCs zur Verfügung, für Unternehmen und Organisationen ist dies kostenpflichtig.

Es scheint aber, als ob die Gefahr trotz allem häufig immer noch unterschätzt wird. „Vor allem Selbständige und Private sparen gerne die Ausgaben für die Sicherheit ein“ (€URO 05 /2004, S.28). Dabei gilt, was Charles Kionga, der Security-Chef der IT-Firma Bechtle, treffend auf den Punkt brachte: “Geeignete Instrumente zur Herstellung von Datensicherheit sind am Markt vorhanden, sie müssen nur genutzt werden“ (€URO 05 /2004, S.27).
Und ist die Entwicklung selbst der wirksamsten Schutzprogramme wirkungslos, wenn sie nicht genutzt werden. Auch ein bewußter und kritischer Umgang mit E-Mails, deren Anhänge

und Downloads gehört zu einer bewußten Gefahreinschätzung. Es ist eben dringend von Nöten, nicht nur mit Sicherheitsprogrammen vorzusorgen, sondern auch aktiv mitzudenken und Gefahren abzuwenden.

Dieser Appell ist umso dringender, als daß die Kosten für die Weltwirtschaft durch die Auswirkungen der Malware in den letzten Jahren Höhen erreicht haben, die jährlich zweistellige Beträge in Milliarden US-Dollar ausmachen. Die in dieser Arbeit genannten Gefahren wie die einer katastrophalen Malware-Attacke weisen auf eine immer stärker zunehmende Bedrohung hin – einhergehend mit einem immer höher werdenden Schadenspotential.

Eine solche Entwicklung ist nicht tragbar. Wie auch immer sich die Computerkriminalität in den nächsten Jahren entwickeln wird, hat sie mit einer harten Strafverfolgung zu rechnen. Sicherheit muß groß geschrieben werden.

Literaturverzeichnis

€URO, Das Magazin für Geld und Wirtschaft, Ausgabe 05 /2004

[1] www.kaspersky.com/de/downloads?chapter=146440562 (01.07.04)
[2] www.heise.de/security/dienste/antivirus/typen.shtml (01.07.04)
[3] www.pc-special.net/?idart=2386 (01.07.04)
[4] www.produktion- net.de/wissen/trendwissen/internet/03_09_03_schaedlingsarten.html (01.07.04)
[5] www.hbedv.de (01.07.04)
[6] viruslist.com/eng/index.html?tnews=1001&id=1614140 (01.07.04)
[7] www.webblitz.de (24.05.04)
[8] www.heise.de/security/news/meldung/47546 (01.07.04)
[9] www.vhs-internet.de/doc/Facharbeit.htm#_Toc3110888 (01.07.04)
[10] www.trendmicro.com/NR/rdonlyres/02A09EAE-3758-41C9-8ED0-1FAF851BA256/2774/realcostwhitepaper.pdf (30.06.04)
[11] www.bowmac.com/it-need.html (01.07.04)
[12] www.astaro.com/data/pdf/whitepapers/Whitepaper_ImprovedNetworkSecurity_en.pdf (24.05.2004)
[13] www.astaro.com/data/pdf/whitepapers/Whitepaper_ImprovedNetworkSecurity_en.pdf (29.06.2004)
[14] www.mi2g.com (01.07.04)
[15] www.bakutoday.net/view.php?d=2358 (24.05.04)
[16] www-personal.umich.edu/~mejn/papers/bfnw.pdf (30.06.04)
[17] www.symantec.com/region/de/depress/download/433istr.zip (30.06.04)
[18] www.imperva.com/docs/Application_Worms.pdf (24.05.04)
[19] www.heise.de/security/artikel/46179 (01.07.04)
[20] www.heise.de/newsticker/meldung/20314 (30.06.04)
[21] www.heise.de/security/artikel/47013 (30.06.2004)