

Seminar-Ausarbeitung

Sicherheit und technischer Datenschutz in Informationssystemen 2006

Angriffe im Netz

Monika Tavas

Universität Karlsruhe

1 Einführung

Zurzeit kann eine steigende Abhängigkeit von der Informationstechnik (IT) in allen Bereichen unseres Lebens beobachtet werden. In Haushalten, sowie in Unternehmen werden die Informationen elektronisch verarbeitet, gespeichert und in Netzen weitergeleitet. Ob Zahlungsverkehr oder auch andere Geschäftsprozesse und Fachaufgaben, alles wird elektronisch gesteuert und bearbeitet. Sämtliche Institutionen aus den wirtschaftlichen Bereichen können mittlerweile ohne IT nicht mehr funktionieren. Nach [fSid06b] werden die IT-Produkte immer kleiner und billiger. Dadurch werden sie immer öfter im Alltag, ohne dass der Konsument es bemerkt, eingesetzt (z. B.: PDAs, RFIDs oder auch integrierte IT- Sensorik in Autos), was laut [fSid06b] zu einer intensiven Verbreitung und Durchdringung von Informationstechnologie führt. Es steigt auch die Vernetzung von IT Systemen. Die Arbeit in IT-Systemen wird nicht mehr isoliert heutzutage durchgeführt, sondern immer stärker vernetzt. In Folge dessen entstehen bessere Kooperationsmodelle und die Arbeitsweise wird globalisiert. In Anlehnung an [fSid06b] führt Globalisierung zum Verschwinden von Netzgrenzen, was durch spontane und drahtlose Kommunikation unterstützt wird. Herkömmliche Unternehmensnetze werden durch die mobilen Computer, Telearbeitsplätze oder drahtlose Übertragungstechnologie wie W-Lan erweitert.

Die starke Vernetzung der IT Systeme und das Verschwinden von Netzgrenzen führen nach [fSid06b] zu Sicherheitsrisiken. Die Zeitspanne zwischen dem Entdecken einer Sicherheitslücke eines Systems und deren Beseitigung wird immer kleiner. Dazwischen kommen schon die ersten Angriffe. Nach [fSid06e] können ausgenutzte Sicherheitsmängel in einem IT-System schnell globale Auswirkungen haben. Beispielweise kann der Zugriff auf Webseiten, die Verwaltungssysteme sowie Support-Seiten unterbrochen werden. Der beste Schutz vor Angriffen aus dem

Netz ist immer noch das Einspielen von Patches und Updates.

Besonders gefährdet sind die kritischen Infrastrukturen¹, wie Behörden, Verwaltung und Justiz, Versorgung, Finanz-, Geld- und Versicherungswesen, Informationstechnik und Telekommunikation, Gefahrenstoffe, Energie oder Transport und Verkehr. Störungen oder Ausfälle in kritischen Infrastrukturen, die im Zusammenhang mit (absichtlich herbeigeführten) Fehlfunktionen der Informationstechnik stehen, können durch eine Kettenreaktion zu weiteren Störungen führen (so genannten Dominoeffekten), die unter Umständen die innere Sicherheit in Deutschland beeinträchtigen können. In der IT und der Telekommunikation als kritischen Infrastrukturen können folgende Bereiche als besonders anfällig erwähnt werden [fSid06a]:

1. Informationserstellung (Messdaten, Berichte, Meldungen etc.)
2. Datenverwaltung und Datenspeicherung (Datenbanken, Server etc.)
3. Informationsverarbeitung (Prozessoren etc.)
4. Informationsübertragung (Vermittlungsknoten)

Laut [fSid06e] steigt mit der Abhängigkeit von der Informationstechnik die Auswirkung des potenziellen Schadens durch den Ausfall der IT - Funktionen. In Anlehnung an [fSid06e] ist der Verlust der Verfügbarkeit, die Vertraulichkeit von Daten, Verlust der Integrität und Verlust der Authentizität gemeint. Durch den Verlust der Verfügbarkeit können keine Geldtransaktionen, Online-Bestellungen und Produktionsprozesse mehr durchgeführt werden. Mit dem Verlust der Vertraulichkeit von Daten werden beispielsweise firmeninterne Daten und personenbezogene Daten nicht mehr vertraulich. Der Verlust der Integrität führt zu dem Verlust der Korrektheit von Daten (zum Beispiel: falsche Entwicklungs- und Planungsdaten oder Fehlbuchungen). Der Verlust der Authentizität ist ein Teil der Integrität. Hier werden Daten falschen Person zugeordnet (z.B. Bestellungen zu Lasten einer dritten Person).

In der Microsoft <kes>-Studie [fSid06d] wurde die Bedeutung der verschiedenen Gefahrenbereiche zur Risikoklassifizierung aufgeführt (siehe Abbildung 1). Seit Beginn der Studie nennen die Teilnehmer hier vor allem „Irrtum und Nachlässigkeit eigener Mitarbeiter“. Weiterhin folgen knapp dahinter als Gefahrenbereiche mit der zweitgrößten Bedeutung Viren, Würmer und Trojanische Pferde (Malware), mit etwa demselben „Abstand“ wie in der vorausgegangenen Studie von 2002. Beides sind gleichzeitig die Risiken, denen die weitaus meisten Befragten zu jeweils über 80% mindestens einen von sechs möglichen Prioritätspunkten zugestanden haben - bei den Plätzen drei bis fünf waren es jeweils 40-50%.

¹Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden [fSid06d].

Gefahrenbereich	Bedeutung heute		Prognose		Schäden	
	Rang	Priorität	Rang	Priorität	Rang	ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	1,50	2	1,70	2	51 %
Malware (Viren, Würmer, Trojanische Pferde usw.)	2	1,34	1	2,80	1	54 %
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	3	0,60	4	1,14	8	9 %
Softwareängel/-defekte	4	0,57	5	0,96	3	43 %
Hacking (Vandalismus, Probing, Missbrauch usw.)	5	0,48	3	1,26	5	9 %
Hardwareängel/-defekte	6	0,40	8	0,32	4	38 %
unbeabsichtigte Fehler von Externen	7	0,30	9	0,26	7	15 %
höhere Gewalt (Feuer, Wasser usw.)	8	0,24	11	0,04	9	8 %
Manipulation zum Zweck der Bereicherung	9	0,17	7	0,43	10	8 %
Mängel der Dokumentation	10	0,15	10	0,20	6	17 %
Sabotage (inkl. DoS)	11	0,12	6	0,55	11	8 %
Sonstiges	12	0,03	12	0,00	12	3 %

Quelle: kes/Microsoft

Abbildung 1: Bedeutung der verschiedenen Gefahrenbereiche für deutsche Unternehmen [fSid06d]

Obwohl das wachsende Gefahrenpotential bekannt ist, stellten laut [fSid06c] im Jahre 2004 nur 39% der deutschen Unternehmen ein höheres Budget zur IT- Sicherheit bereit, bei 40% stagnierte der Etat. 2005 belegte die ICISA Labs Studie([do-PR06]), dass die Häufigkeit der Angriffe durch Virus-Attacken in Unternehmen und die Kosten zu ihrer Schadensbeseitigung bereits gestiegen sind. Nach neuesten Studien von VDEB ([dESu06]) wurden die Investitionen zur IT-Sicherheit weltweit um 95% erhöht.

2 Angriffe im Netz

Im folgenden Kapitel werden verschiedene Arten von Angriffen im Netz beschrieben. Alle können als Manipulation bezeichnet werden, die „eine vorsätzliche Änderung oder Gestaltung eines Objektes in der Regel zum Schaden oder Nachteil des Eigentümers, des Besitzers oder des Benutzers“ [Dier05] bedeutet. In Zusammenhang mit IT-Systemen und deren Komponenten werden nach [Dier05] folgende Elemente als Manipulationsobjekte bezeichnet: Programme, Bauteile oder Baugruppen, Rechner und deren Peripherie, Daten, Programm-Generatoren, Versorgungseinrichtungen und Infrastruktur, Netze und Netzkomponenten.

Es ist umstritten, wem und wie durch die Manipulation die „Schäden“ entstehen. Von daher soll laut [Dier05] im Vordergrund in der Definition der Manipulation die ordnungsmässige Funktion des Systems stehen. Das bedeutet, dass nach einer Manipulation ein System oder ein Systemteil nicht ordnungsmässig funktioniert (Fehlfunktion). Somit wird eine verallgemeinerte Definition der Manipulation relevant:

Manipulation ist jede vorsätzliche Änderung oder Gestaltung eines Objekts für die gilt:

Ist \neq Soll

Ein Beispiel einer berühmten Manipulation ist das trojanische Pferd ² aus der Ilias des Homer.

Zu den wichtigsten Programmanomalien und -manipulationen gehören: Fehler, Trojanisches Pferd, Verschleierungsprogramm, Logische Bombe, Hintertür, Wurm und Virus.

²Odysseus hatte schon von Anfangs an vor, das hölzerne Pferd (in IT -Programm) mit einer Schadfunktion auszustatten, nämlich die Griechen die im Inneren versteckt sein sollten. Die Funktion wurde dem Trojaner (heutigen Anwender) natürlich nicht verraten. Das Objekt wurde als nützlicher Gegenstand gesehen, als „Geschenk der Götter“(in Bezug auf IT- als Computerspiele, nützliche Tools, usw.).

2.1 Fehler

In Anlehnung an [Dier05] wird ein Fehler (eng. bug) als Programm oder Programmteil mit Wirkungen, die nicht den Anforderungen entsprechen, bezeichnet. Er kann schon bei dem ersten Entwurf von Anwendung eingebracht werden. Die Verursacher von Fehlern können Menschen sowie Programme selbst sein (Compiler, Programmgenerator, usw.).

Da die heutige Software sehr komplex ist, treten laut [fSid06f] sehr oft Programmierfehler ein. Es ist zu beobachten, dass hohe Erwartungen der Anwender und zeitlich zu knapp bemessene Erscheinungstermine bei Standardsoftwareprodukten auch dazu führen, dass die Hersteller ihre Produkte teilweise unausgereift oder nicht fehlerfrei anbieten. Werden diese Softwarefehler nicht erkannt, können die bei der Anwendung entstehenden Fehler zu weitergehenden Folgen führen.

Fehler lösen nach [Dier05] die gleiche Wirkung wie Manipulationen aus. Das System funktioniert nicht ordnungsgemäss. Infolgedessen kann für die Fehler auch die Manipulationsdefinition benutzt werden, falls das Wort vorsätzlich gestrichen wird. Somit kann die Manipulation als eine spezielle Art von Fehler bezeichnet werden, bei der die „von den Anforderungen abweichende Wirkung ausdrücklich gewollt ist“ [Dier05].

Fehler bei Software-Produkten sind für die Hacker wie eine offene Tür zum System. In Anlehnung an [Gerw06] stellte im Jahre 2004 das Microsoft-Produkt „Windows Explorer“ ein gutes Beispiel dar. Um die Benutzerfreundlichkeit des Programms zu steigern, wurden für die Sicherheit relevante Informationen nicht angezeigt. Bei den Voreinstellungen waren zum Beispiel Datei-Endungen nicht angezeigt. Der Windows Explorer kannte auch nicht den Unterschied zwischen Ausführen und Anzeigen. Er laut [Gerw06] kannte nur „Öffnen“/„Anklicken“. Somit konnte der Anwender eine exe Datei ausführen, ohne es zu wissen.

Ein anderes Beispiel stellten nach [Gerw06] die echten Sicherheitslücken der Internet Explorer dar. Mit Hilfe von einfachen Tricks war es möglich die E-Mails auszuführen ohne den schädlichen Anhang des Mails zu öffnen. In den letzten zwei Jahren hat Microsoft die Fehler beheben können.

2.2 Trojanisches Pferd

Für [Dier05] ist das trojanische Pferd(engl. Trojan horse) ein Programm oder ein Programmteil mit verdeckten Wirkungen (oder Nebenwirkungen). Der Trojaner bietet nach [Wiki06c] eine nützliche Anwendung, wobei im Hintergrund ohne Wissen des Anwenders eine andere Funktion (z.B.: Virus, Wurm) abläuft. Das Trojanische Pferd verbreitet sich entweder über Datenträger oder im Internet (Tauschbörsen, E-Mail).

Trojaner können nach [Wiki06c] und [ddSe06] die Benutzerdaten ausspionieren, Tastaturenfolgen zeichnen und zum Autor des Trojanischen Pferdes weiterleiten. Andere Funktionen beziehen sich auf das Überwachen von Home-Banking-Programmen, ständige Anzeige von unerwünschter Werbung, die Weiterleitung auf be-

stimmte Webseiten, das Ausspionieren von Passwörtern für Online-Dienste/ Mail Accounts/ Webseiten/ FTP/ Kreditkarten-Nr., Konten usw.

Die gefährlichsten trojanischen Pferde stellen laut [ddSe06] so genannte Serverprogramme dar. Sie ermöglichen dem Hacker den Zugriff auf das System. Das Programm kann die Tastaturfolgen aufzeichnen, Passwörter auslesen, herunter- und/oder hochladen von Dateien von/auf betroffene Systeme. Der Hacker hat mitunter vollen Zugriff auf den Rechner. Server-Programme bestehen aus einem Clienten (dieser wird benutzt um auf andere Systeme zugreifen zu können) und dem eigentlichen Trojaner, dem Server. Trojaner unterscheiden sich je nach ausgeführter Tätigkeit. Nach [abIn06b] werden die Trojaner folgendermassen aufgeteilt:

- **Backdoor-Trojaner-Utility der Remote-Administrierung:** Ermöglichen die entfernte (remote) Administrierung von Computern im Netz
- **Trojan-PSW - Passwort-Diebstahl:** Beim Start suchen die PSW-Trojaner nach System-Dateien, die diverse vertrauliche Informationen enthalten (meist Telefon-Nummern oder Kennwörter, die den Zugang zum Internet gewährleisten) und senden diese an die im Trojaner-Code angezeigten E-Mail-Adressen.
- **Trojan-Clicker - Internet-Klicker:** Die Hauptfunktion dieser Trojanerfamilie ist die Organisierung ungesetzmässiger Zutritte zu Internet-Ressourcen (meist zu Webseiten).
- **Trojan-Downloader - Zustellung anderer Schadprogramme:** Diese Trojaner sind zur Installation von neuen Schadprogramm-Versionen, von 'Trojanern' und Reklame-Systemen auf Opfer-Computern vorgesehen.
- **Trojan-Dropper - Installateur anderer Schadprogramme:** Trojaner Programme dieser Klasse installieren versteckt andere Programme und werden praktisch immer dafür genutzt, um auf einen Opfer-Computer Viren oder Trojaner zu schleusen
- **Trojan-Proxy - Trojaner Proxy-Server:** Diese Familie der Trojaner organisiert versteckt anonymen Zugang zu verschiedenen Internet-Ressourcen. Gewöhnlich verwenden sie dafür Spam-Versand.
- **Trojan-Spy - Spion-Programme:** Diese Trojaner führen eine elektronische Spionage des Anwenders der infizierten Maschine durch: die über die Tastatur eingegebene Information, Monitor-Abbildungen (Screenshots), Listen der aktiven Programme und der Aktivitäten des Anwenders werden in irgendeiner Datei auf der Festplatte gespeichert und in bestimmten Abständen an den Übeltäter versandt.
- **Trojan-Notifier - Meldung über eine erfolgreich durchgeführte Attacke:** Diese Trojaner sind dafür vorgesehen, dem 'Eigentümer' über den infizierten

Computer zu berichten. Dafür wird an die Adresse des 'Eigentümers' eine Information über den Computer gesandt - z.B. die IP-Adresse des Computers, die Nummer des offenen Portals, die E-Mail-Adresse u.a. Der Versand erfolgt auf verschiedene Weise, beispielsweise über E-Mail oder ISQ.

Um sich vor Trojanern schützen zu können, sollten nach [Wiki06c] die Anwender auf die Benutzung von Programmen aus unbekanntem oder unsicheren Quellen verzichten. Auch Antivirensoftware und Firewalls sollten eingesetzt werden. Die Antivirensoftware ist wirkungsvoll vor dem Ausführen des Trojaners, danach könnte die Erkennungsrate nicht immer vollständig sein. [Wiki06c] besagt, dass die Firewalls zwar vor dieser Art von Schadprogrammen nicht schützen, jedoch können sie auf unautorisierte Netzwerkkommunikation hinweisen. Nach Möglichkeit sollten laut [Pern06] die Passwörter nicht auf der Festplatte gespeichert werden und der Zugang zu sensiblen Daten sowie Anwendungen sollten auf ein Minimum beschränkt werden.

2.3 Verschleierungsprogramm

In Anlehnung an [Dier05] ist das Verschleierungsprogramm (engl. spoofing program) ein Programm oder ein Programmteil, der die Oberfläche oder das Verhalten einer bekannten (System)-Funktion vorspielt. Er gehört zu den trojanischen Pferden und stellt sich als bekanntes und beliebtes Programm (Spiel, Werkzeug, usw.) dar. Anstelle der bekannten Funktion wird jedoch eine ganz andere Funktion ausgeführt.

Als Beispiel dafür nennt [Dier05] die LOGON Prozedur. Ein Hacker schreibt ein Programm, das sich genauso wie LOGON verhält. Der Benutzer tippt seine UserId ein und gibt sein Passwort ein. Es erscheint eine „Systemantwort“: „*LOGON unsuccessful — incorrect password*“.

Der Benutzer gibt noch einmal sein Passwort und denkt, dass er sich zuvor lediglich vertippt hat. Inzwischen wird das Passwort und die Benutzer-Id in die Datei des Hackers geschickt und gespeichert.

Ähnlich können viele solche Verschleierungsprogramme für z.B. Funktionen aus der Textverarbeitung oder graphischen Datenverarbeitung geschrieben werden.

Als Schutzmassnahmen bietet [Pern06] die Programmauthentifikation mit „digitalem Fingerabdruck“ an. Auch die Code-Inspektion mit Hilfe von Programmen, die Modifikationen am Quellcode feststellen wird als eine gute Lösung erwähnt.

2.4 Logische Bomben, Zeitbomben

Die Logische Bombe/ Zeitbombe ist nach [Dier05] eine Art des trojanischen Pferdes, das seine versteckte zerstörerische Wirkung erst nach Eintreten eines bestimmten Ereignisses (Auslöser) entfaltet. Auslöser ist eine Abfrage einer Bedingung (siehe Abbildung 2). Je nachdem, ob die Abfrage innerhalb des Systems beantwortet und bearbeitet werden kann, oder noch zusätzliche Informationen von aussen geliefert werden müssen, können interne und externe Auslöser unterschieden werden.

```
Subroutine AUSLÖSER ::=  
{if Datum > 3.7.2006 then 'true'  
 otherwise 'false'}
```

Abbildung 2: Mechanismus eines Zeitauslösers

Zu internen Auslösern gehören laut [Dier05] die Datums- und Zeitangaben, Zähler und interne Ereignisse. Bei Daten- oder Zeitangaben handelt es sich um eine Abfrage wie in Abbildung 2 von Kalender/Uhr, die als festes Element in jedem System eingebaut sind. Das Hacker Programm läuft dann z. B. einmal täglich, oder wird in einem trojanischen Pferd verstreckt, das mehrmals täglich aufgerufen wird. Als Zähler kann der Hacker die Anzahl von Systemstarts (boots) oder die Anzahl der Aufrufe der bestimmten Systemteile einsetzen. Klassische Beispiele für die internen Ereignisse sind Prozeduraufrufe, Zugriffe auf bestimmte Dateien, sowie Aufrufe von bestimmten Unterprogrammen oder Systemfunktionen.

Als externen Auslöser nennt [Dier05] die Schlüssel- oder Passwörter, externe Ereignisse, Transaktionen und Ausbleiben von Ereignissen (Toter-Mann-Knopf³).

Als Schlüssel oder Passwort wird eine bestimmte Buchstaben-Reihenfolge erwartet. Die Ereignisse in der Kommunikation des Systems mit seiner Umwelt lösen externe Ereignisse und Transaktionen aus, zum Beispiel der Aufruf einer Transaktion oder einer Systemfunktion von der Eingabe aus. Alternativ kann das Ausbleiben von Ereignissen auch zum Auslöser der Bombe werden. Bezeichnung dafür ist der Toter- Mann- Knopf.

2.5 Hintertüren, Falltüren

Gemäss [Dier05] ist die Hintertür(engl. Trap door) ein Programm oder ein Programmteil mit verdeckten oder unbekanntem Nebenein- oder Nebenausgängen. Ein Hacker oder ein aktives Element versucht durch die geheimen oder unbekanntem Lücken in einem Programm oder einem System einzudringen. Die Hintertüren sind alle Arten von Befehlen, Programmteilen, Systemkomponenten, die für den ordnungsgemässen Betrieb nicht benötigt werden und trotzdem vorhanden sind. Allerdings sollten die besonderen Funktionen für bevollmächtigte Benutzer wie Wartungspersonal, Systemprogrammierer nicht dazu gerechnet werden. Sie werden laut [Pern06] oft von Programmierern (legal) implementiert (aber nicht dokumentiert), um während der Entwicklung z.B. langwierige Authentifikationsprozesse beim Debuggen zu vermeiden und das Programm zu aktivieren, wenn etwas mit der Authentifizierung nicht funktionieren sollte.

Die Beispiele für die Hintertüren sind verschiedene Unterbrechungsvektoren im Betriebssystem MS-DOS. In Versionen die bis jetzt auf dem Markt erschienen sind,

³im Eisenbahnwesen: wenn in bestimmten Abständen ein Knopf nicht gedrückt wird, wird eine Notbremung ausgelöst

wird lediglich die Hälfte der Unterbrechungsvektoren benutzt. Laut [Dier05] war das Brain - Virus , bekannt auch als Pakistani⁴, ein typisches Beispiel für Hintertüren, welches ungenutzte Befehle des Systems ausgenutzt hat. Es benutzte einen ungenutzten Befehl im Betriebssystem - Unterbrechungsvektor 6H.

Ähnliche Gefahren stellen nach [Dier05] alle User Exits dar. Dies sind die Schnittstellen in System und Systemteilen, bei denen der User seine eigenen Programmteile anbinden kann und somit eine Benutzerfreundlichkeit des Systems schafft. Dies kann jedoch zu einer Sicherheits- Katastrophe im System führen, falls die Schnittstelle nicht genau durchdacht wurde.

2.6 Wurm

Für [Dier05] ist der Wurm (engl. worm) ein Programm, das sich selbst reproduziert und in einem System selbständig ablaufen kann [Dier05]. Nach [Shoc82] kann ein Wurm auf einem oder mehreren Rechner leben und aus verschiedenen Segmenten bestehen, die versuchen miteinander zu kommunizieren. Er verbreitet sich über Computernetzwerke, mit Hilfe von Wirtsapplikationen, Netzwerkdiensten oder Benutzerinteraktionen.

Ein Beispiel dafür stellen infizierte E-Mails, ISQ-, IRC-, Peer - To -Peer - Programme, usw. dar. 2004/05 wurden laut [Wiki06b] die ersten Handy-Würmer entdeckt, die sich durch Bluetooth und MMS verbreiten.

Würmer können je nach Verbreitungsart, Installation und anderen eigenen Merkmalen unterschiedlich kategorisiert werden. [abIn06a] klassifiziert sie in zwei Hauptkategorien: E-Mail Worms-Postwürmer und Internet Worms-andere Netzwürmer. Die Postwürmer verbreiten sich laut [abIn06a] als Anhang an den elektronischen Brief, oder einen Link auf seine Datei, die sich auf einer beliebigen Netzressource befindet.

Sie nutzen verschiedene Methoden zum Absenden infizierter Nachrichten. Unter anderem den direkten Anschluss an den SMTP-Server, MS-Outlook-Service oder direkten Anschluss an den SMTP-Server. Um beispielweise die Adressen der E-Mails zu finden, zählen die Würmer die Adressen aus der WAB-Adress-Datenbank oder scannen die 'passenden' Dateien der Festplatte und heben die Zeilen hervor, die E-Mail-Adressen darstellen. Würmer können darüberhinaus sich selbst an alle Adressen senden, die sie in den Briefen aus der Mailbox gefunden haben (wobei einige der Postwürmer in der Mailbox gefundene Briefe „beantworten“). Zu den Postwürmern gehören Instant Messaging (ICQ und MSN) Worms und IRC Worms

⁴Es wurde von zwei Brüdern aus Pakistan geschrieben, deren Absichten bis heute nicht bekannt sind und eine Firma „Brain Computer Services“ besaßen. Es ist möglich, dass in Pakistan Raubkopien legal waren und die Brüder durch den Virus das eigene Produkt schützen wollten. Denkbar ist ebenfalls die absicht die „Opfer“ des Virus an sich zu binden ([Lupo06]). Brain-Virus war der erste MS-DOS Virus. Er überschrieb den Bootsektor einer Diskette, verschob den originalen Bootsektor an eine andere Stelle auf der Diskette und schrieb sich selbst in zwei ergänzende Sektoren. Er besetzte also 3 Sektoren und bediente sich dafür des ungenutzten Platzes auf der Diskette. Wenn der Bootsektor beispielsweise beim Starten gebraucht wurde, las der Virus den originalen Bootsektor, am neuen Speicherort, ab und wurde so getarnt.

- Würmer in den IRC-Kanälen.

Nach [abIn06a] verbreiten sich die Internet Worms-andere Netzwürmer durch Kopieren auf die Netzressourcen, Ausnutzung von den Schwachstellen im Betriebssystem und Dienstprogrammen oder auch durch Eindringen in die Netz-Ressourcen zur öffentlichen Nutzung. Es ist möglich, dass ein Wurm auch mehrere Infektionsmethoden benutzt. Zu den Internet Worms gehören File-sharing Networks oder P2P Worms - Würmer für Datei-Austausch-Netze. Hier verbreiten sich die Würmer durch Kopieren in einen freigegebenen Ordner, von dem andere Benutzer Dateien downloaden können oder der Wurm kopiert sich in das gesuchte Datei, die als Ergebnis der Suchabfrage erscheint.

Um sich vor den Würmern schützen zu können, sollten nach [abIn06a] die Software auf neusten Stand gebracht werden (besonders Betriebssysteme und E-Mail-Software), Virens Scanner eingesetzt werden und keine unbekannt E-Mails geöffnet werden. Durch regelmäßige Updates werden die bekannten Sicherheitslücken beseitigt. Vor der Installation einer Software oder einer Funktion sollten alle Informationen bezüglich Sicherheit bekannt werden. Es ist nach [Wiki06b] auch ratsam, sich Gedanken zu machen, ob eine auffällige Anwendung weiter eingesetzt werden soll oder nicht. Es ist sinnvoll, Personal - Firewalls einzusetzen. Sie können Anfragen über das Netzwerk an laufende Server-Anwendungen ausfiltern und das Ausnutzen von nicht bekannten Sicherheitslücken verhindern. Auch den Zugriff auf bestimmte Arten von Attachments (z.B. .vbs, .exe Datei) sollte laut [Pern06] unterbunden sein.

2.7 Virus

Ein Virus (engl. virus) ist nach [Dier05] ein nicht-selbständiger Programmcode mit der Eigenschaft der Infektion. Er reproduziert Code und manipuliert ein Wirtsprogramm (oder dessen Umgebung) so, dass mit dessen Nutzung auch das Virusprogramm abläuft. Im Gegensatz zu Würmer verbreitet sich das Virus nicht von Computer zu Computer, sondern von Datei zu Datei. Nach [fSid06a] besteht das Virus aus Reproduktions-, Erkennungs-, Schadens-(optional), Bedingungs-(optional) und Tarnungsteil. Der Reproduktionsteil dient zur Vermehrung des Virus. Mithilfe des Erkennungsteils wird geprüft, ob eine Datei schon infiziert wurde. Jedes Wirtsprogramm wird nur einmal infiziert, was zur schnellen Ausbreitung des Virus führt. Manche Viren haben einen eingebauten Schadensteil, der auch einen Auslöser(z. B. Abfrage, Datum) besitzen kann. Die schädliche Funktion kann z.B. Programme und Daten überschreiben, verändern oder löschen. Sie kann ebenfalls die Ausgabe von Meldungen oder Geräuschen verursachen. Diese Schadensfunktion kann auch fehlen. Allerdings kann das Virus trotzdem den Schaden verursachen durch die Belegung von Hauptspeicherplatz. Der Ausbruch oder die Verbreitung des Virus kann vom Bedingungssteil abhängen, falls er vorhanden ist. Der Tarnungssteil erschwert die Entdeckung des Virus. Er ist jedoch nur in neueren Viren zu finden [fSid06a]. Eine typische Struktur eines Virus zeigt Abbildung 3. Das Hauptprogramm des Virus ruft zunächst das Unterprogramm für die Vermehrung-“Infektion“, daraufhin

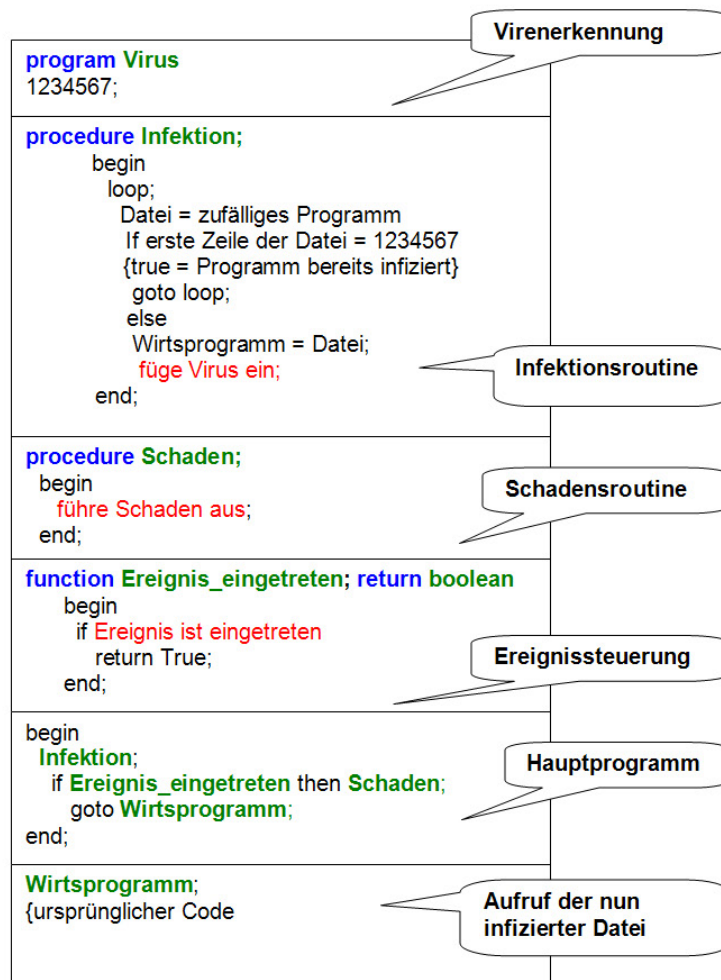


Abbildung 3: Typische Struktur des Virus nach [Pern06]

ruft er nach der Erfüllung der entsprechenden Bedingung die schädliche Funktion auf, und springt danach zurück, in der Regel in das Wirtsprogramm, d.h. in dasjenige Programm, in das das Virusprogramm sich eingemischt und von wo aus es seine Wirkung entfaltet hat.

Nach [Dier05] kann leicht erkannt werden, dass die Infektion und die (schädliche) Funktion sich unterscheiden. Durch die Infektion folgt die Vermehrung und Ausbreitung der Viren. In diesem Prozess können zwei Unterprozesse erkannt werden: Reproduktion des Viruscodes und Manipulation eines Wirtsprogramms oder seiner Umgebung. Die Infektion kann direkt oder indirekt erfolgen. Bei der direkten Manipulation werden die Teile des Viruscodes in das Wirtsprogramm integriert oder der Wirts-Code wird überschrieben, was zur Aufteilung in nicht-überschreibende und überschreibende oder komprimierende Viren führt. Bei in-

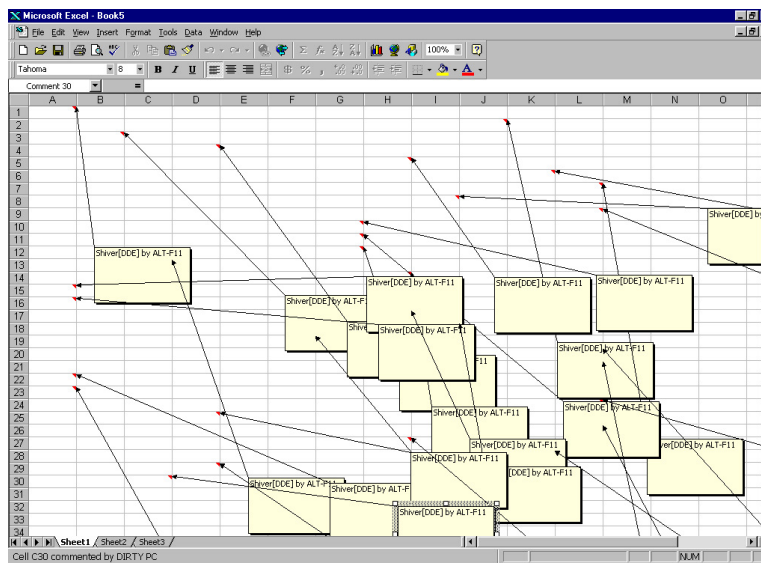


Abbildung 4: Ein Makro-Virus

direkter Manipulation laut [Dier05] wird die Umgebung der zu manipulierenden Programme geändert. Beispiele dafür stellen die Boot-Sektor-Viren (der Startsektor des Betriebssystems wird verändert) oder die Directory-Viren (Dateiverzeichnisse werden „verborgen“) dar.

Eine besonders unangenehme Art von Viren stellen nach [Dier05] die Makro-Viren dar, bei welchem ein Viruscode als „Hilfsprogramm“ in Texte und Schriftstücke eingebettet wird (siehe Abbildung 4). So ist es möglich von Word aus unbemerkt die Festplatte zu formatieren.

Viele Viren können keiner speziellen Kategorie zugeordnet werden. Beispielsweise können sie Dateien und Bootsektoren infizieren. Heute ist schon fast jede Variation möglich. In Anlehnung an [Wiki06a] werden sie als Mischformen von Viren bezeichnet.

Prävention kann nach [Wiki06a] durch Installation einer Antivirensoftware folgen. Sinnvoll ist das Umbenennen von wichtigen Dateien (FORMAT.com, FDISK.EXE). Es sollte Zugang zu sensiblen Daten und Anwendungen beschränkt werden und Verschlüsselung von Daten und Anwendungen erfolgen. Die Ausführung von Makros sollte auf ein Minimum beschränkt werden.

Die Personal Firewall zeigen keine Wirkung gegen diese Art von Angriffen. Grundsätzlich sind alle Betriebssysteme für Viren anfällig. Am anfälligsten laut [Wiki06a] sind MS-DOS, Windows 9x und Amiga-Systeme. Die weitest verbreiteten Windows Systeme stellen auch das beliebteste Ziel von Viren-Autoren dar. Es sind 60.000 Viren für Microsoft Systeme bekannt. Die Zahl der Viren für Linux und Mac OS liegt bei ca. 50. Die Top Viren zeigt die Abbildung 5. Die gefährlichsten Viren sind Mytob (31%), Netsky(23%) und Mydoom(12,5%)

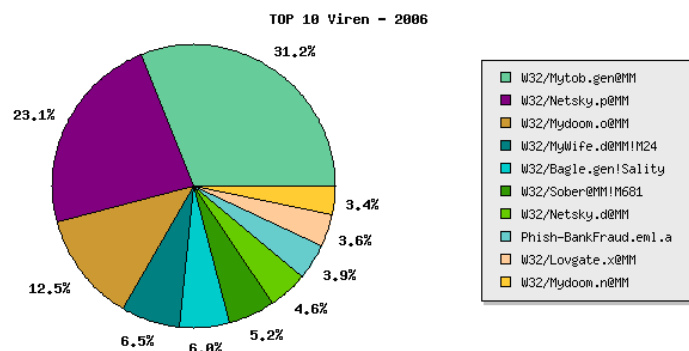


Abbildung 5: Die Top Viren in 2006

3 Schwachstellen und Bedrohungen in IT Systemen

In Anlehnung an [fSid06c] haben im Jahre 2004 die Schadprogramme (83,1%) die grösste Bedrohung von IT-Systemen dargestellt (siehe Abbildung 6). 30,4% wurden durch die Schwachstellen in Systemen verursacht.

Heute ist Ähnliches gegeben. Fakt ist, dass die Schadprogramme immer effektiver programmiert werden. Laut [fSid06c] ist ein Grund dafür eine starke Verbreitung von standard Softwares und Monokulturen bei Betriebssystemen. Computerwürmer werden immer öfter dazu programmiert den Computer unter Kontrolle zu bringen anstatt den Schaden anzurichten, was zu einer steigenden Anzahl der DoS - Angriffe führt.

Ausserdem hat sich nach [fSid06c] in letzten Jahren das Problem der Spionagesoftware wie Spyware und Adware entwickelt. Sie sammeln die Informationen ohne Wissen des Anwenders. Mit Hilfe von Spyware können Passwörter und Kontonummer ausspioniert werden. Durch die Adware werden die Nutzungsgewohnheiten des Anwenders aufgezeichnet und zu Marketingzwecken weiter verkauft. Schützen kann man sich durch regelmässige Sicherheitsupdates, Verwendung aktueller Antivirensoftware, sowie Benutzung der Firewall. Auch Deaktivierung der Ausführung von ActiveX-Steuer-elementen und der Speicherung von Third Party Cookies in den Browsereinstellungen ist hilfreich.

Gegen die Internetserver führen die Hacker gezielte Angriffe, so genannte Dos-Attacken (engl. Denial-of-Service). Der Angreifer überflutet laut [fSid06c] den Server mit sinnlosen Paketen und überlastet das System. Dadurch können die Kunden auf die Waren und anderen Informationen nicht zugreifen. In Zusammenhang stehende organisierte Attacken mit mehreren Computer von Dritten heissen Denial-of-Service-Attacken (DDoS). Die Attacken werden nicht gegen Opfer sondern gegen Internetanbieter durchgeführt. DDoS Angriffe stellen in Anlehnung an [fSid06c] eine ernste Bedrohung für die Web-Server dar. Sie können sogar zu Server-Ausfällen führen, wie z.B. im Januar 2006 durchgeführte DDoS-Angriffe gegen Server von milliondollarhomepage.com, die einen sechs tätigen Ausfall des Servers verursacht haben. Nach [Möll06] gehören zu den Schutzmassnahmen ge-

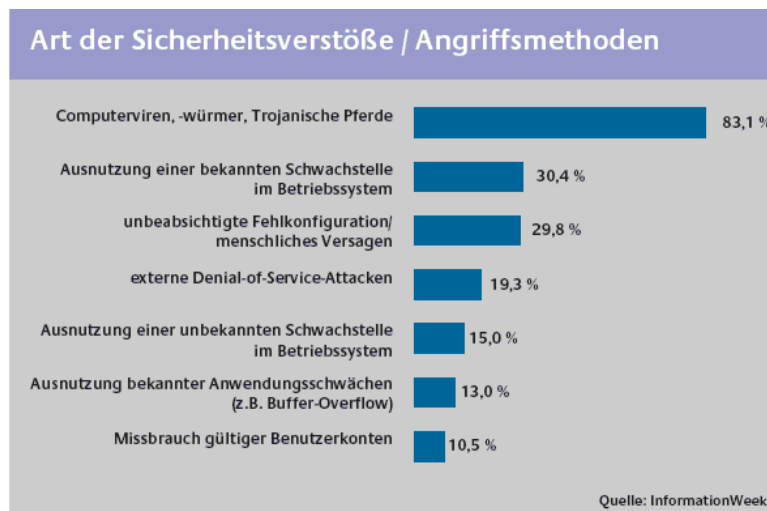


Abbildung 6: Verbreitung von Angriffsmethoden in deutschen und schweizerischen Unternehmen [Info]

gen DDoS der Aufbau eines Systems zur Verfolgung von Datenströmen in Netzen, Scannen nach DDoS Komponenten, Abschalten von Directed-Broadcasts, Verwendung von Verschlüsselung für Authentifikation und Kommunikation, Einschränkung der angebotenen Dienste auf den notwendigen Netzbereich, zeitnahe Einspielen von Sicherheitspatches oder konservative Systemkonfiguration. Leider setzen die Internetprovider laut [fSid06c] zu selten gezielte Schutzmassnahmen gegen die Bekämpfung dieser Art von Angriffen.

Hier ist es interessant zu bemerken, dass im Jahr 2004 viele der registrierten Trojanischen Pferde die Funktionen für koordinierte Angriffe gegen Internetserver übertragen haben. Mithilfe dieser Methode wird die Zahl von kontrollierten Computern und die Schlagkraft eines verteilten Dos-Angriffes schnell erhöht.

Die infizierten Computer bilden dann die Bot-Netze, die jeder Zeit für Angriffe und Erpressung von Unternehmen einsetzbar sind. 2004 haben die Netze über 30.000 Computer erreicht. Durch Einführen des Windows-XP-Service-Packs 2 von Microsoft ist die Anzahl von infizierten Computern auf 5000 gesunken.

Die Spams stellen auch ein Problem dar. [fSid06c] besagt, dass seit 2001 der Anteil der Spam- E-Mails stark zugenommen hat. 2001 waren 21% und 2005 bereits zwei Drittel aller E-Mails ein Spam. Für die Zukunft wird laut [Pern06] ein weiterer Anstieg des Spam-Anteils vorhergesagt. Infolge der grossen Anzahl von solchen Nachrichten kommt es zu Arbeitszeitausfällen, zur Überlastung technischer Komponenten und zu höheren Kosten für unerwünschten Datenverkehr. Spams, genauso wie Viren und Würmer werden durch die Massenmailwürmer, die den infizierten Computer durchsuchen, verschickt. Nach [Pern06] wären 2005 direkte Schäden in Höhe von ca. 158 Mrd. Euro entstanden, wenn es nicht die Technologien und Konzepten gegen Spam gäbe. Trotz der hohen Anzahl an verschickten Spams pro Tag,

werden laut [fSid06c] die Antispammassnahmen noch nicht vollkommen umgesetzt.

In den vergangenen 2 Jahren wuchst nach [Pern06] die Anzahl der Phishings - Mails. Die E-Mails werden mit einer gefälschter Absenderadresse versehen. Über einen Link in der E-Mail wird der Anwender auf die gefälschte Webseite eines bekannten Unternehmens geleitet. Dadurch versuchen die Betrüger die Passwörter und Konto-Nummern für das Online-banking auszuspionieren. Der durchschnittliche Schaden pro Phishing -Fall beläuft sich auf etwa 150 Euro. Insgesamt ergeben die direkten und indirekten Schäden von Phishing etwa einen zweistelligen Milliarden Euro Betrag, wobei eine genaue Schätzung nicht möglich ist.

Um Kunden vor Phishing zu schützen, bieten Banken laut [Pern06] oftmals proprietäre Software anstelle der browserbasierten Funktion für das Online-Banking an. Von einigen Banken umgesetzt sind TAN Verfahren, in denen anstatt einer vom Nutzer gewählten TAN eine bestimmte TAN aus einem Block verlangt wird. Gegen Phishing E-Mails kann man sich als User genauso schützen wie vor SPAM-Mails. Technische Ansätze sind sehr wenig ausgereift. Erste Firmen wie z.B. die Mozilla Foundation haben begonnen, Tools gegen Phishing zu entwickeln.

4 Trends und Entwicklung bei IT-Bedrohungen

Abgesehen von den in Kapitel 2 und Kapitel 3 beschriebenen Angriffen erfolgen immer neue zielgerichtete Angriffe durch Hacker. Der Hauptgrund dafür ist eine schnelle Entwicklung von IT-Produkten und des Marktes. Es nimmt die Zahl von Wirtschaftsspionage zu. Laut [fSid06c] sind Technologie und Know-how die klassischen Ziele des Diebstahls. Es werden die Ausschreibungen, Verträge oder die Preisinformationen ausspioniert, um die Wettbewerbsvorteile zu steigern. Das Ausspähen von Unternehmensdaten wird nach [fSid06c] in den nächsten 10 Jahren deutlich zunehmen. Eigene Mitarbeiter oder Outsourcing-Mitarbeiter stellen auch ein Gefahropotenzial dar. Sie haben einen schnellen Zugang zu den sensiblen Daten oder der Einblick in interne Sicherheitsstrukturen eines Unternehmens. Der Verlust von Vertraulichkeit (siehe Kapitel 1) von Daten kann zu schweren wirtschaftlichen Schäden des Unternehmens führen, wie z. B. einem schlechten Image der Firma. Am stärksten sind Forschung und Entwicklung betroffen. Ein weiteres Problem stellen gerichtete Angriffe gegen Infrastrukturen dar. Es kann ein rapider Anstieg von Angriffen auf die Namenserver beobachtet werden. Die Internetnutzer können durch diese manipulierten Server massenhaft auf gefälschte Phishing-Webseiten fehlgeleitet werden. Laut [Syma06] zielten 16 Prozent der Hackeraktivitäten auf E-Commerce-Unternehmen, was im Vergleich zum 2004 einem Zuwachs um 400 Prozent entspricht. Der Trend für das Ausspionieren von Kreditkarteninformationen und anderen sensitiven Finanzdaten wird sich laut [fSid06c] weiter verstärken. Ebenfalls ein grosses Sicherheitsproblem stellen gezielte DDoS-Angriffe (Kapitel 2) gegen Unternehmen dar. Ursachen sind oft die Konkurrenz, unzufriedene Mitarbeiter oder anders motivierte Personenkreise. Nach [fSid06c] kann auch ein

Trend bei Internetkriminalität beobachtet werden, der in Richtung Professionalisierung und Kommerzialisierung führt. Anstelle isolierter Computerhacker steht hinter gerichteten Angriffen vermehrt die organisierte Kriminalität. Hacker und Virenautoren arbeiten mit den Kriminellen zusammen und schreiben Schadprogramme für Phishing, Kreditkartenbetrug und Erpressungstricks. An dieser Stelle kann der finanzielle Reiz als ausschlaggebend für die Tätigkeiten angesprochen werden. Durch den Missbrauch von IT-Systemen lässt sich nach [fSid06c] mittels der Verbreitung von Spam sowie des Missbrauchs sensibler Daten wie Kreditkartennummern oder Onlinebankingdaten Geld verdienen. Eine Zunehmende Regionalisierung von Schadprogrammen führt dazu, dass die E-Mails, die Computerwürmer enthalten, sind in deutsch geschrieben. Diese Regionalisierung führt zu einer weiten Verbreitung solcher Schadprogramme in Deutschland.

Literatur

- [abIn06a] Viruslist.com alles über Internet-Sicherheit. Network Worms - Netzwerkwürmer, August 2006.
- [abIn06b] Viruslist.com alles über Internet-Sicherheit. Trojaner-Programme, August 2006.
- [ddSe06] Trojaner Info die deutsche Security Seite. Trojanische Pferde- was ist das?, August 2006.
- [dESu06] Verband der EDV-Software und Beratungsunternehmen e.V. IT - Markt, August 2006.
- [Dier05] Rüdiger; S.M. Dierstein. Programm-Manipulationen - Arten, Eigenschaften und Bekämpfung, 2005.
- [doPR06] OpenPR das offene PR Portal. ICSA Labs Studie belegt alarmierende Eskalation der Auswirkungen von Virus-Attacken, August 2006.
- [fSid06a] Bundesamt für Sicherheit in der Informationstechnik. Informationen zu Computer-Viren, August 2006.
- [fSid06b] Bundesamt für Sicherheit in der Informationstechnik. IT-Grundschutz - Basis für IT-Sicherheit, August 2006.
- [fSid06c] Bundesamt für Sicherheit in der Informationstechnik. Lage der IT - Sicherheit in Deutschland 2005, August 2006.
- [fSid06d] Bundesamt für Sicherheit in der Informationstechnik. Schutz Kritischer Infrastrukturen in Deutschland, August 2006.
- [fSid06e] Bundesamt für Sicherheit in der Informationstechnik. Sicherheit im Internet, August 2006.

- [fSid06f] Bundesamt für Sicherheit in der Informationstechnik. Software-Schwachstellen oder -Fehler, August 2006.
- [Gerw06] Peter Gerwinski. Nein, ich habe Ihnen keinen Virus/Wurm/Spam geschickt!, August 2006.
- [Info] InformationWeek. IT- Security 2004.
- [Möll06] S. Möller, K.; Kelm. Distributed Denial of Service Angriffe, August 2006.
- [Pern06] Günter Pernul. Vorlesung an der Universität Regensburg Informatik Bestiarium, August 2006.
- [Shoc82] J.A. Shoch, F./ Hupp. The Worm Programs: Early Experience with a Distributed Computation. Communications of the ACM 25, 1982.
- [Syma06] Symantec. Internet Security Threat Report, August 2006.
- [Wiki06a] die freie Enzyklopädie Wikipedia. Computervirus, August 2006.
- [Wiki06b] die freie Enzyklopädie Wikipedia. Computerwurm, August 2006.
- [Wiki06c] die freie Enzyklopädie Wikipedia. Trojanisches Pferd (Computerprogramm), August 2006.