Computerwurm

Ein **Computerwurm** ist ein Computerprogramm, das sich über Computernetzwerke verbreitet und dafür so genannte „höhere Ressourcen“, wie Netzwerkdienste oder eine Benutzerinteraktion, jedoch kein Wirtsprogramm, benötigt. Es verbreitet sich zum Beispiel durch das Versenden infizierter E-Mails (selbstständig durch eine SMTP-Engine oder durch ein E-Mail-Programm), durch IRC-, Peer to Peer- und Instant-Messaging-MMS.

. Die Klassifizierung als Wurm bezieht sich hierbei auf die Verbreitungsfunktion.

Ein Wurmprogramm muss nicht unbedingt eine spezielle Schadensroutine enthalten. Da das Wurmprogramm aber sowohl auf den infizierten Systemen als auch auf den Systemen, die es zu infizieren versucht, Ressourcen zur Weiterverbreitung bindet, kann es allein dadurch erhebliche wirtschaftliche Schäden anrichten. Des Weiteren können Würmer die Belastung anderer Systeme im Netzwerk wie Mailserver, Router und Firewalls erhöhen.

Laut einer Untersuchung von Sophos, eines Herstellers von Anti-Viren-Software, bestand im Jahr 2005 eine 50-prozentige Wahrscheinlichkeit für einen neuen PC mit Windows XP ohne Aktualisierungen, im Internet innerhalb von zwölf Minuten mit schädlicher Software infiziert zu werden. Insbesondere durch die in späteren Windows-Versionen standardmäßig aktivierte Firewall und den vermehrten Einsatz von SoHo-Routern hat sich diese Gefahr zwar verringer, ist jedoch durch neue Angriffsvektoren weiterhin gegeben.

Unterschied zwischen Virus und Wurm

Computerviren und -würmer verbreiten sich beide auf Computern, doch basieren sie zum Teil auf verschiedenen Konzepten und Techniken. Ein Virus verbreitet sich, indem es Dateien infiziert, also sich in eine ausführbare Datei, in einigen Fällen auch in einen Bootsektor oder als Makro in eine interpretierbare Datei integriert und somit Teil einer schon bestehenden Programmroutine wird. Die Verbreitung des Virus erfolgt durch Weitergabe dieser infizierten Dateien. Auf welchem Wege sie weitergegeben werden (über Datenträger oder Netzwerke), ist für die Definition „Virus“ unerheblich. Der Unterschied zum Computerwurm besteht einerseits darin, dass ein Virus sich autark verbreitet, da die oben erwähnte Abhängigkeit zur „höheren Ressource“ nicht besteht.

Würmer warten andererseits nicht passiv darauf, dass sie mit infizierten Dateien weitergegeben werden. Sie versuchen auf unterschiedliche Art, aktiv via Netzwerk weitere Computer zu infizieren. Aber auch ein Wurm kann – wie ein Virus – in vertrauenswürdigen Dateien getarnt integriert sein, in diesem Fall hat man evtl. beide Übertragungsarten und daher eine Mischform. Als dritte Art gibt es noch die Trojaner (Trojanisches Pferd), diese bezeichneten vor der Verbreitung des Internets Programme, die einen Nutzen vortäuschten, aber eine Schadroutine beinhalteten. Beispielsweise ein Prüfungstool für Disketten, das selber sogenannte Bad Sectors produzierte, anstatt sie zu erkennen. Obwohl diese Trojanischen Pferde sehr selten waren, wurden sie bereits von den ersten Antivirusprogrammen als Schadsoftware erkannt. Heute wird der Begriff „Trojaner“ fast ausschließlich für Backdoor-

Programme gebraucht, die sich vor allem dadurch auszeichnen, dass sie eine Hintertür auf dem System installieren, über welche die Versender (etwa die Programmierer) Zugriff auf den kompromittierten Rechner haben. Heutzutage sind häufig Mischformen (Trojanerwürmer und Trojanerviren) anzutreffen.

Tarnung und Verbreitung

Würmer verbreiten sich derzeit meistens entweder über E-Mails oder über Netzwerke. In seltenen Fällen werden diese auch als Download oder integriertes Objekt auf Webseiten angeboten. Diese Methode hat aber den Nachteil, dass der Betreiber einer Webseite kaum anonym bleiben kann.

Einmal aktiviert durchsucht die Schadsoftware die Adresslisten und Kontakte des E-Mail-Programms und versendet automatisch an alle gefundenen Adressen eine E-Mail mit sich selbst als Anhang, ohne dass der Benutzer es merkt. In diesem Zusammenhang sind insbesondere die Microsoft-Produkte – oder die auf einem Microsoft-Betriebssystem aufbauenden E-Mail-Programme – auffällig geworden. Jedoch sind auch andere Betriebssysteme und Clients angreifbar und haben vom Anwender ungewollt und vollautomatisch Schadcode verbreitet. Je mehr Möglichkeiten ein Wurm hat, sich weiterzuversenden, desto erfolgreicher kann er sich verbreiten.

Da der Computerwurm selbst ein ausführbares Programm darstellt (ob nun als Binärdatei oder in Form eines durch eine andere Anwendung zu interpretierenden Quelltextes), ist er darauf angewiesen, entweder vom Benutzer ausgeführt zu werden, oder durch eine Sicherheitslücke im Zusammenhang mit dem Empfang des Computerwurms automatisch ausgeführt zu werden. Da Sicherheitslücken eher selten sind und bei funktionierender Unterstützung durch den Hersteller zumeist auch relativ schnell geschlossen werden, kommt der Verbreitung von Schadcode durch Bequemlichkeit, Unwissenheit und mitunter auch fahrlässiges Fehlverhalten des Benutzers selbst eine nicht zu unterschätzende Bedeutung zu.

Ausführung durch den Benutzer

Der Wurm wird als E-Mail-Anhang empfangen. Der Empfänger soll nun veranlasst werden, den Anhang zu öffnen und somit eine Infektion auszulösen. Dies kann unter zwei sich ergänzenden Voraussetzungen erfolgen:

- Der Empfänger der E-Mail muss ein besonderes Interesse daran haben, den Anhang zu öffnen.
- Der Empfänger darf sich der Gefährlichkeit des Anhangs nicht bewusst werden.

Die hier verwendeten Methoden greifen eigentlich den Benutzer des EDV-Systems an, nicht das System selbst.

Psychologische Beeinflussung des Empfängers

Das Interesse des Empfängers am Anhang wird erweckt, wenn der Inhalt der dazugehörigen E-Mail entweder auf eine besondere Schockwirkung abzielt, indem beispielsweise mit Rechtsmitteln bis hin zur Strafverfolgung gedroht wird. Andere Begleittexte versuchen,

Neugier oder Begierden zu erwecken, indem hohe Geldbeträge versprochen oder vermeintlich private Bilddateien mit oder ohne pornographischem Inhalt angeboten werden. In jedem Fall wird der Empfänger auf den Anhang der E-Mail verwiesen, welcher ausführliche Informationen enthalten soll. Das so geweckte Interesse am Dateianhang dämpft naturgemäß auch eventuelle Sicherheitsbedenken (*siehe auch:* Social Engineering).

Tarnung durch doppelte Dateinamenserweiterung

Wurmprogrammdateien werden mit doppelter Dateinamenserweiterung versehen, wobei darauf gebaut wird, dass beim Empfänger die Anzeige der Dateinamenerweiterung für bekannte Dateitypen ausgeblendet wird (Windows-Standardeinstellung). So wird beispielsweise eine ausführbare Anwendung „music.mp3.exe“ unter Windows nur als „music.mp3“ angezeigt. Somit erscheint es dem Opfer zunächst als harmlose Musikdatei.

Der Anwender könnte den wahren Dateityp jedoch erkennen, da das angezeigte Dateisymbol (Icon) dem Standardsymbol einer Anwendung entspricht. Eine Anwendung zum Abspielen von Multimediadateien kann eine derartig getarnte ausführbare Datei ebenfalls nicht öffnen, reagiert also mit einer Fehlermeldung.

Lange Dateinamen

Die Verwendung eines unverdächtigen, aber äußerst langen Dateinamens (etwa *private_bilder_meiner_familie_aus_dem_sommercamp_nordsee_2003.jpg.exe*) soll über die Dateinamenerweiterung hinwegtäuschen. Da der Dateiname zumeist in einem relativ kleinen Dialogfenster angezeigt wird, bleibt der letzte Teil des Dateinamens und somit die Erweiterung verborgen. Eine zusätzliche Tarnung wird erreicht, indem als Dateiname zunächst ein kurzer, unverdächtiger Name mit falscher Dateinamenerweiterung verwendet wird, an den eine Vielzahl von Leerzeichen vor der echten Erweiterung eingefügt sind (etwa *ihre_Daten.doc .exe*). Dadurch erscheint in einem kleinen Dialogfenster kein Hinweis mehr auf den eigentlich erheblich längeren Namen.

Wenig verbreitete Typen von ausführbaren Dateien

Da Anwendungen des Typs .exe als ausführbare Dateien relativ bekannt sind, wird mitunter auch auf weniger verbreitete Dateitypen (Dateiformate) zurückgegriffen:

- Dateitypen, welche vor allem als Systemkomponenten zum Einsatz kommen und deshalb von unerfahrenen Benutzern wenig beachtet werden (Beispiele: .dll, .ax, .ocx).
- Dateien, welche mitunter auch als nichtausführbare Formate auftreten können (Beispiele: .dll, .scf, .ini).
- Dateitypen, welche durch andere Dateitypen abgelöst wurden und deshalb weniger gebräuchlich geworden sind (Beispiele: .com, .pif, .bat). Die Dateiendung .com ist zudem geeignet, einen Link auf eine Internet-Seite vorzutäuschen (z. B. www.namexyz.com).

Komprimierung

Durch die Verwendung von Komprimierungsformaten (ZIP) wird einerseits der Dateityp verschleiert und andererseits die Anwendung automatischer Schutzvorkehrungen erschwert bis umgangen. Da moderne Virenscanner auch in Archiven komprimierte Dateien analysieren

können, wird auch mit Verschlüsselung gearbeitet, was aber mitunter den Argwohn des Benutzers wecken könnte. Alternativ kann auch zunächst ein mehrfach komprimiertes übergroßes Archiv gesendet werden, um den Virenscanner durch Überlastung auszuschalten.

Automatische Ausführung

Eine von außerhalb auf ein EDV-System übertragene Datei kann von der betreffenden Systemkomponente oder der auf diesem System befindlichen Übertragungssoftware sofort geöffnet werden. Üblicherweise ist dies aber nicht vorgesehen. Internetbrowser arbeiten darüber hinaus in einer sogenannten „Sandbox“, welche als zusätzliche Abschirmung dienen soll. Wenn dies nicht so wäre, könnte auf einer Internetseite einfach die Dos-Kommandozeile *format c:* als Link eingebaut werden.

Tatsächlich bestehen aber Sicherheitslücken, vor allem deshalb, weil einige Funktionen vorgesehen sind, welche der Bequemlichkeit des Anwenders dienen sollen, aber die üblichen Sicherheitseinschränkungen durchbrechen. Hierzu gehören die automatische Ausführung von Anwendungen, welche als „Objekte“ in eine Webseite oder ein HTML-E-Mail eingebunden sind.

Da die Architektur der Microsoft-Systeme eine hohe Proprietät und eine Orientierung an einem bestimmten Nutzerprofil aufweist, ergeben sich hier besonders häufig Sicherheitsprobleme. Die Verwendung von ActiveX-Objekten, welche von außerhalb aktiviert werden können, sowie die Implementierung von JScript und VBScript als relativ mächtige Scriptsprachen kann eine gewisse Benutzerfreundlichkeit ermöglichen, birgt aber hohe Risiken. Letztlich müssen bestimmte, vom Entwickler eigentlich gewollte Funktionen blockiert werden, um übliche Sicherheitsstandards zu erfüllen. Dabei kann es hin und wieder zu Fehlern kommen, welche bei der Verbreitung von Malware genutzt werden können.

Der Wurm *MS Blaster* nutzt einen Remote-Exploit in der RPC/DCOM-Schnittstelle von Windows 2000 und XP. Das bedeutet, er nutzt eine Sicherheitslücke aus (engl. „to exploit“), um Rechner über Netzwerke zu infizieren. Nach einer Infektion beginnt er, wahllos Netze (also z. B. das Internet) nach weiteren Rechnern mit dieser Sicherheitslücke abzusuchen, um sie unverzüglich ebenfalls zu infizieren (*siehe auch:* Geschichte der Computerwürmer).

Neben Sicherheitslücken des Betriebssystems können auch Sicherheitslücken in Anwendungssoftware Einfallstore für Würmer bieten. Eine Reihe von Würmern nutzt einen Fehler im E-Mail-Programm Microsoft Outlook Express. Die Anlagen von HTML-E-Mails werden von Outlook Express üblicherweise *inline*, also direkt in der Nachricht selbst, dargestellt. Alternativ kann der Quelltext der E-Mail auch eine Referenz enthalten, unter welcher die betreffende Datei online hinterlegt ist, und dann in einem Inlineframe dargestellt wird. Innerhalb eines HTML-Quelltextes können Dateiformate, welche nicht dem Internetstandard entsprechen und deshalb normalerweise nicht direkt in eine HTML-Seite eingebunden werden können, als „Objekte“ definiert werden. Dazu wird dem System mitgeteilt, welcher Art das „Objekt“ ist und wie das System damit zu verfahren hat. Der HTML-Parser *mshtml.dll* müsste jetzt abfragen, ob diese Art von „Objekt“ bekannt ist und ausgeführt werden darf. Offensichtlich ist diese Abfrage der Schwachpunkt des Systems, da eine bestimmte fehlerhafte Abfrage zu einem Systemfehler und daraufhin zur Ausführung des „Objektes“ führt, obwohl das Gegenteil zu erwarten wäre. Allein das Betrachten

des E-Mail-Textes startete also—ohne weiteres Zutun des Anwenders—die Schadsoftware. Dieser Fehler ist bei allen Versionen des Internet Explorers so oder ähnlich aufgetreten. Jedes Mal, so auch jetzt, wurde der Fehler durch eine Aktualisierung behoben. Eine ähnliche Sicherheitslücke existierte auch im E-Mail-Programm „Eudora“.

Auch speziell für den Angriff auf Servercomputer konzipierte Würmer sind bekannt. So spezialisierte sich in der Vergangenheit eine ganze Reihe von Würmern auf Sicherheitslücken im *Internet Information Services* (weit verbreitete Webserver-Software für Windows). Nach der Infektion begannen die Server selbstständig nach weiteren Servern zu suchen, um auch diese zu infizieren.

Instant-Messaging-Würmer

Instant-Messaging-Programme wie zum Beispiel ICQ oder MSN Messenger sind durch ihre Web- Anbindung ebenfalls anfällig für Malware. Ein Wurm dieser Art verbreitet sich, indem an einen Messenger ein Link zu einer Internetseite geschickt wird, welche den Wurm enthält. Klickt der Benutzer auf den Link, wird der Wurm auf dessen Computer installiert und ausgeführt, da der Instant-Messenger zumeist keinen eigenen HTML-Parser enthält, sondern den Parser des Internet-Explorer mitnutzt. Nun sendet der Wurm von diesem Computer den Link an alle eingetragenen Kontakte weiter.

P2P-Würmer

Peer-to-Peer ist eine Netzwerkform, die ohne Server Rechner im Netz verbindet, d. h. eine Direktverbindung zwischen den einzelnen Benutzern herstellt. Die meisten im Internet bestehenden Tauschbörsen wie Kazaa, Morpheus oder BitTorrent Systeme nutzen Peer-to-Peer-Technologie. Es gibt im Großen und Ganzen drei Möglichkeiten, wie sich ein Wurm in einer Tauschbörse verbreitet.

Die erste Möglichkeit ist, dass sich der Wurm in den freigegebenen Ordner kopiert, von dem andere Benutzer Dateien herunterladen können. Für diese Art von Würmern ist die richtige Namensgebung wichtig, da mehr Benutzer eine Datei mit einem interessanten Namen herunterladen als eine Datei mit einem zufällig erstellten Namen. Darum gibt es Würmer, die ihre Namen im Internet auf speziellen Seiten suchen, um so glaubwürdig wie möglich zu sein. Diese Art der Verbreitung in Tauschbörsen ist einfach, aber nicht besonders effektiv, da in Tauschbörsen üblicherweise eher große Dateien getauscht werden und fast jedes Filesharing-Programm inzwischen wirksame Filter besitzt, um bestimmte verdächtige Dateiformate auszugrenzen.

Bei der zweiten Möglichkeit der Verbreitung bietet der Wurm über ein Peer-to-Peer-Protokoll bei jeder Suchabfrage den anderen Benutzern des P2P-Netzwerkes eine infizierte Datei als Suchergebnis (Hashset oder .torrent- File) an. Der Benutzer kopiert dann den Wurm als vermeintlich gesuchte Datei auf seinen Computer und infiziert ihn beim Öffnen. Diese Art der Verbreitung ist sehr effektiv, sofern die Dateigröße des Wurms annähernd so groß ist wie die gesuchte Datei, aber schwierig zu programmieren und deshalb kaum verbreitet.

Die dritte und gefährlichste Methode, der sich ein Wurm bedienen kann, um sich in einem P2P-Netzwerk zu verbreiten, ist ein automatisierter Angriff des Wurms auf alle

Nachbarn im P2P-Netzwerk. Diese Methode ist deshalb so gefährlich, weil zum einen keine Aktion seitens des Benutzers (wie das Herunterladen einer Datei und deren Ausführen auf dem Rechner) benötigt wird. Der Wurm greift automatisiert eine Sicherheitslücke im P2P-Programm an und infiziert dieses dadurch. Zum anderen ist der Wurm in der Lage, sich rasend schnell zu verbreiten, da er bei jedem infizierten Client eine Liste seiner Nachbarn im P2P-Netzwerk vorfindet, die er dann angreifen kann. Dadurch kann der Wurm auch einer Entdeckung vorbeugen, da „normale“ Würmer eine große Anzahl an Verbindungen zu anderen Systemen im Internet aufbauen, was als anormales Verhalten angesehen wird. Ein P2P-Netzwerk basiert aber darauf, dass jeder Nutzer viele Verbindungen zu anderen Teilnehmern aufbaut, was die Erkennung des Wurms anhand des von ihm verursachten Traffics deutlich erschwert.