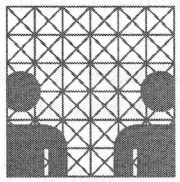
Impressum
Universität Hamburg
Fachbereich Informatik
Virus-Test-Center
Vogt-Kölln-Straße 30
22527 Hamburg

Telefon: ☎040 / 42883 - 2234 (Labor)
☎040 / 42883 - 2405 (Sekretariat)

Fax: ☎040 / 42883 - 2226

Web-Seite: http://agn-www.informatik.uni-hamburg.de



VTC VIRUS TEST CENTER

Viren und Malware

Eine Einführung

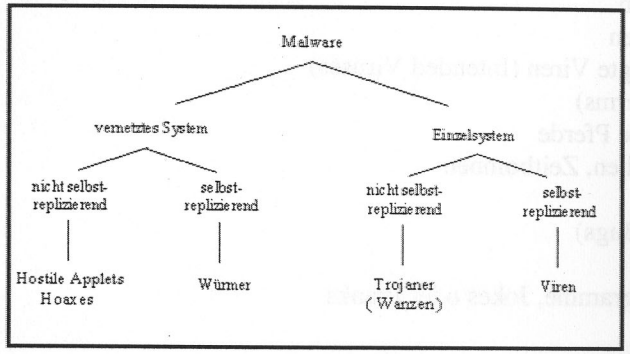
Inhaltsverzeichnis

Was ist Malware?

Mit dem Begriff „Malware“ wird allgemein bösartige Software bezeichnet.

Als Oberbegriff umfaßt er alle Arten maliziöser Software, sei es nun selbst-replizierende (Viren und Würmer) oder nicht-selbst-replizierende (u.a. Trojanische Pferde, Hostile Applets, Hoaxes, Dropper).

Die Abbildung verdeutlicht die Stellung der einzelnen Begriffe in Bezug auf ihre Fähigkeit zur Selbst-Replikation und die Eigenschaft, Einzelrechner oder ganze Netze zu ihrer Verbreitung zu nutzen.



Ergänzend sei noch erwähnt, daß natürlich auch Viren und Trojaner mit Hilfe von Computernetzen, insbesondere dem weltweiten Internet, rege Verteilung erfahren. Dies ist aber keine charakteristische Eigenschaft, denn anders als etwa Würmer benötigen sie keine Netzwerke zur Verbreitung.

Die Problematik des Begriffes „Malware“

Einzig beim Begriff des Virus existiert ein eindeutiges Kriterium, anhand dessen sich von einem vorliegendem Stück Software entscheiden läßt, ob es den Begriff erfüllt, nämlich die Fähigkeit der Selbstreplikation.

Bei den anderen Formen der Malware hängt die Beurteilung, ob ein Programm als „böswillig“ bezeichnet werden darf oder sollte, von einer Vielzahl von Randbedingungen ab, die nicht am Programm selbst ablesbar sind.

Wie im Abschnitt über Trojanische Pferde erläutert, kann diese Entscheidung unter anderem davon abhängen, welche Erwartung ein Benutzer an ein Programm hat, das er ausführen möchte.

Definition des Begriffes Computervirus:

Ein Computer-Virus ist ein in ein Wirtsprogramm eingebettetes oder mit einem Wirtsprogramm verbundenes, sich selbst reproduzierendes Computerprogramm bzw. Stück ausführbarer Programm-Code.
Zur Reproduktion modifiziert der Virus andere Programme in einer Weise, daß diese dann eine (möglicherweise abgewandelte) Kopie seiner selbst enthalten. Bei Aufruf des Wirtsprogramms erfolgt eine Ausführung des Virus. Dies kann und soll (aus der Sicht des Viren-Autors) eine Ausbreitung des Virus bewirken.

Diese Definition umfaßt auch die Kategorie der System- und Makroviren, da wir auch den im Master Boot Record (enthält Partitionstabelle der Festplatte), im Bootsektor und in Dokumenten vorhandenen ausführbaren Code als Wirtsprogramm verstehen.

Aufbau eines Virus:

Der Installationsteil installiert den Virus nach seinem Aufruf im Hauptspeicher des Computers, vielfach wird hierbei auch getestet, ob der Virus bereits im Speicher aktiv ist. Verfügt der Virus über Funktionen zur Selbsttarnung, mit denen er sein Vorhandensein zu kaschieren versucht, so sind diese hier angesiedelt.

Im Reproduktionsteil finden sich die Anweisungen zum Kopieren und damit zur Vermehrung des Virus. Die Bestimmung eines Infektions-Opfers kann von unterschiedlichen Auswahlkriterien abhängig gemacht sein.

Die Payload bzw. der Schadensteil ist nicht Teil der Definition des Begriffes „Virus“, da sie nicht zwingend in einem Virus vorhanden sein muß. Bezeichnet wird damit der Teil des Virus, der Funktionen enthält, die nicht mit dem Replikationsprozeß in Zusammenhang stehen.

Viele der tatsächlich auftretenden Viren beschränken sich auf das bloße Vervielfältigen und Ausbreiten ihrer selbst. Allerdings stellt auch das Wirken eines solchen Virus alleine durch das Verändern von Dateien, das Belegen von Speicherplatz im Hauptspeicher und auf der Festplatte oder Disketten sowie durch die Verlangsamung des Systems

durch die Beanspruchung von Rechenkapazität eine „Schädigung“ dar.

Ist die Payload aber vorhanden, gibt es für sie eine Vielzahl von Möglichkeiten, ein Computersystem zu schädigen. Die Ausführung der Schadensfunktionen, wie z.B. das Formatieren der Festplatte, wird in der Regel vom Erfülltsein einer bestimmten Bedingung abhängig gemacht, um dem Virus Zeit zur Ausbreitung zu geben, bevor er durch den bewirkten Schaden auffällt oder das System inklusive sich selbst unbrauchbar macht.

Grundtypen der Malware:

Systemviren (Bootviren)

Dieser Typus von Viren benutzt als Wirt keine Anwendungsprogramme, sondern infiziert das System selbst.
Disketten und Festplatten, von denen ein Computer gebootet werden kann, enthalten in Systembereichen ausführbaren Code, der beim Systemstart ausgeführt wird. Diese Tatsache nutzen diese Viren aus, indem sie ihren eigenen Code dorthin schreiben und somit zuverlässig zur Ausführung gelangen.

Dateiviren

Dateiviren verbreiten sich über die Infektion ausführbarer Dateien.

Wird ein mit einem Virus infiziertes Programm aufgerufen, wird zunächst der Virus ausgeführt. Um dies zu erreichen, kann der Virus verschiedene Strategien verfolgen:

Wenn er seinen Hauptcode an das Ende der Datei anhängt, muß er den Anfang des Wirtsprogramms durch einen Sprungbefehl zu seiner eigenen Startadresse ersetzen. Die ersten Befehle des Originalprogramms werden an einer anderen Stelle gespeichert.

Nach Beendigung der Ausführung des Viruscodes führt der Virus dann zuerst diese Anfangsbefehle des Wirtsprogramms aus und verzweigt dann zurück an den ursprünglichen Programmstart, um das Originalprogramm normal ablaufen zu lassen.

Viren, die nach dieser Methode vorgehen, werden „Anhängende Viren“ („Appending Viruses“) genannt.

Eine andere Methode der Infektion ist es, einfach den Anfang des Wirtsprogrammes mit dem Viruscode zu überschreiben, wodurch das Programm aber zerstört wird. Diese „Überschreibenden Viren“ können aber dadurch schneller auffällig werden, weil die befallenen Programme nicht mehr lauffähig sind.

Schließlich kann ein Virus auch versuchen, in den Opferdateien unbenutzte Freiräume zu suchen, in die er seinen Code einbetten kann. Die Wirtsdateien verändern sich bei einer Infektion durch diese sogenannten „Cavity“-Viren nicht in ihrer Länge, und verraten sich auf diese Weise nicht durch geänderte Dateigrößen.

Companion-Viren

„Companion - Viren“ lassen ihre Opferdateien unberührt und erreichen ihre Ausführung anstelle der betroffenen Datei, indem sie ihren Code in einer neu erzeugten Datei ablegen, die dann anstelle des vom Benutzer aufgerufenen Programms ausgeführt wird. Zum Ende seines Ablaufes ruft der Virus die Opferdatei auf, damit die Manipulation nicht auffällt.

Um dies zu erreichen, wird unter DOS die neue Virusdatei als COM-Datei mit dem gleichen Namen wie die zu befallende EXE-Datei abgelegt. Bei einem Aufruf des Programmes ohne die Angabe der Dateierweiterung wird dann die COM-Datei mit dem Virus ausgeführt, weil der Kommandointerpreter von DOS bei der Angabe eines Dateinamens ohne Endung immer zuerst nach einem Programm dieses Namens mit der Endung „COM“ sucht. Nur wenn eine solche nicht vorhanden ist, wird nach den Endungen „EXE“ und „BAT“ weitergesucht.

Findet sich die aufgerufene Datei nicht im aktuellen Verzeichnis, so durchsucht der Kommandointerpreter von DOS alle Verzeichnisse, die im Suchpfad eingetragen sind (angegeben in der „AUTOEXEC.BAT“-Datei).

Dabei geht er in der Reihenfolge vor, die in der Path-Variable festgelegt ist. Ein „Path-Companion-Virus“ nutzt dieses Verhalten aus, indem er Kopien von sich in weiter vorne stehenden Pfaden ablegt.

Die „Renaming-Companion“-Viren benennen die Originaldatei um und geben der Virusdatei den ursprünglichen Dateinamen. Das hat dann zur Folge, daß nun auch bei Angabe des kompletten Dateinamens inklusive Dateierweiterung der Virus anstelle des angesprochenen Programmes ausgeführt wird.

Unter einem Betriebssystem mit grafischer Oberfläche wie Windows 95/98/NT zeigen nun alle Verknüpfungen statt auf die Programmdatei auf den Virus und werden ihn gegebenenfalls aufrufen.

Dateisystemviren

Um das Ziel zu erreichen, daß der Virus vor oder anstelle eines anderen Programmes ausgeführt wird, manipulieren Dateisystemviren die Verzeichniseinträge des Dateisystems derart, daß die Verzeichniseinträge nicht länger auf das Programm, sondern auf den Virusanfang verweisen. Nur wenige Viren funktionieren nach diesem Prinzip.

Multi-Partite-Viren

Diese Mischform von Datei- und Bootsektor-Viren kann gleichermaßen Dateien und auch Bootsektoren bzw. Master-Boot-Records infizieren. Die Verbreitung kann also sowohl über die Weitergabe von infizierten Dateien als auch von infizierten Datenträgern erfolgen.

Makroviren

Einige moderne Anwendungsprogramme wie Word oder Excel von Microsoft besitzen Dateiformate die nicht nur (formatierte) Texte oder Daten enthalten, sondern auch ausführbaren Code, die sogenannten Makros. Makroviren sind in solch einer Makro-Programmiersprache geschrieben und infizieren im Gegensatz zu Dateiviren nicht direkt ausführbare Programme, sondern Dokumentdateien der entsprechenden Anwendung.

Zur Ausführung gelangen diese Viren schon beim einfachen Öffnen eines infizierten Dokumentes in der Anwendung. Die Makroprogrammiersprachen enthalten nicht nur Funktionen des zugehörigen Anwendungsprogramms, sondern auch Kommandos, um Funktionen des Betriebssystems anzusprechen, was den Makroviren umfangreichen Zugriff auf viele Systemkomponenten ermöglicht. Da die Lauffähigkeit der Makroviren lediglich von der unterstützten Makrosprache abhängig ist, sind diese Viren von der Rechner-Plattform und dem Betriebssystem unabhängig.

Skript-Viren

Diese Viren befallen Skripte wie JavaScript oder VBScript (VisualBasic-Script), die z. B. mit Hilfe des WSH (Windows Scripting Host) ausgeführt werden. Sie sind im Gegensatz zu Skript-Würmern noch selten.

Beabsichtigte Viren (Intended Viruses)

Solche Dateien sind nicht (richtig) funktionierende Programme, die vom Programmierer als Viren geplant waren, aber so schwerwiegende Programmfehler enthalten, daß etwa die Infektion anderer Dateien oder Systembereiche fehlschlägt oder die zweite Generation dieses Nicht-Viruses sich nicht mehr replizieren kann.

Keime (Germs)

Dies sind Viren in der ursprünglichen Form, so wie sie vom Autor kommen. Die Datei ist so gestaltet, daß die Infektion nicht auf normale Weise stattgefunden haben kann, oder es handelt sich um eine Kopie des Virus ohne eine Wirtsdatei.

Trojanische Pferde

Mit dem Ausdruck Trojanisches Pferd oder einfach Trojaner werden Programme bezeichnet, die neben einer vom Benutzer erwarteten und gewünschten Funktionalität noch weitere, verborgene und unerwünschte Funktionen erfüllen.

Diese zusätzliche Funktionalität, die auf verschiedene Weise schädlich sein kann, sei es in einer zerstörerischen Wirkung oder auch durch das ausspähen von Informationen, wurde vom Programmierer beabsichtigt und stellt aus seiner Sicht den eigentlichen Zweck des Programmes dar, der sich hinter der vorgeblichen, für den Benutzer nützlichen Funktion verbirgt. Diese nützliche Funktion kann von dem Programm trotzdem erbracht werden, um ein mehrfaches Ausführen zu erzielen. Falls die verborgene Funktion in ihrem Verhalten so auffällig ist, daß sich das Trojanische Pferd dabei als solches verrät, etwa durch das Ausführen einer Schadensroutine, ist es letztendlich für den „Erfolg" des Trojanischen Pferdes nicht notwendig, daß es die versprochene Leistung auch tatsächlich erbringt.
Besonderes Augenmerk in der Definition des Begriffes des Trojaners sollte auf der Bedingung dessen, was der Benutzer erwartet, liegen.

Viele Handlungen, die ein Computerprogramm ausführen kann, sind nur abhängig von dem Kontext, in dem sie ausgeführt werden, als schädlich oder nicht schädlich anzusehen. Das Formatieren einer Festplatte kann ebenso gewollt, wie auch sehr unerwünscht sein.

Durch das reine Betrachten des Programmcodes einer Software läßt sich nicht entscheiden, ob es sich um einen Trojaner handelt oder nicht. Bestenfalls läßt sich eine potentiell gefährliche, potentiell unerwünschte Funktionalität feststellen, die ein Programm als mögliches Trojanisches Pferd qualifiziert.

Trojanische Pferde sind nicht selbst-reproduzierend und können selbständige Programme sein.

Weil ein Trojaner relativ einfach zu programmieren ist und auch ein primitiv programmiertes Trojanisches Pferd trotzdem seinen Zweck erfüllen kann, gibt es noch mehr mangelhaft funktionierende Exemplare als bei den Viren, jedoch ist der Trend zu beobachten, daß die tatsächlich auftretenden Trojaner immer professioneller programmiert werden. Während es sich anfangs hauptsächlich um spielerische, einfach gemachte Programme handelte, führt das Internet mit seinen zahlreichen Verbreitungsmöglichkeiten dazu, daß auch die nicht selbst-replizierende Malware (wieder) an Relevanz gewinnt.

Gründe dafür sind darin zu sehen, daß zum einen mit den relativ neuen Java-Applets und Active-X-Controls neue Methoden zur Verbreitung von Trojanern entstanden sind und sich zum anderen mit dem wachsendem Bereich des Online-Bankings neue Motivationen für betrügerische Manipulationen ergeben.

Logikbomben, Zeitbomben

Eine „Bombe“ führt eine bestimmte, schädliche Handlung aus, wobei die Ausführung abhängig gemacht wird von der Erfüllung einer bestimmten Bedingung (des „Triggers“).
Demnach sind Bomben als „getriggerte Trojaner“ als Spezialfall des Trojanischen Pferdes anzusehen.
Nach Art des Triggers kann man die Bomben einteilen in folgende Untertypen:

Ist der Trigger eine logische (boolesche) Bedingung, spricht man von einer Logik-Bombe (oder auch „logische Bombe“).

Bei Zeitbomben stellt eine zeitliche Bedingung die Trigger-Variable dar. Signalbomben warten auf ein bestimmtes Signal, bevor sie ihren Schadensteil ausführen.

Oft sind Bomben Teil eines größeren Programmes.

Dropper

Dies ist eine spezielle Variante eines Trojanischen Pferdes. Als verborgene Funktion enthält ein Dropper die Fähigkeit, einen Virus oder ein Trojanisches Pferd zu installieren. Der Dropper selbst ist kein Virus, da er sich selbst nicht replizieren kann. Er ist auch nicht mit dem Virus, den er trägt, infiziert. Installiert der Dropper den Virus nur im Speicher und nicht auf einem Datenträger, so nennt man ich auch „Injector“.

Wanzen (Bugs)

Als Wanzen oder Bugs bezeichnet man Fehler in der Software, die beim Entwurf oder der Implementation entstanden sind. Das fehlerhafte Programm verhält sich deshalb anders als vom Programmierer beabsichtigt und damit anders als vom Benutzer erwartet, diese Mängel entstehen in der Regel unabsichtlich und stellen keine böswillige Attacke dar. Sie können sich auch nicht selbst verbreiten.

Hoaxes

Hoaxes sind falsche Warnmeldungen über nicht wirklich existierende Viren oder Trojaner, die überwiegend im Internet verbreitet werden, um Panik unter den Computerbenutzern zu verursachen.
Sie werden weiterverbreitet, weil viele Empfänger einen Hoax nicht von einer richtigen Virenwarnung unterscheiden können und sie zur Warnung an Bekannte weitergeben.

Scherzprogramme, Jokes oder Pranks

Diese Programme tun etwas, was den Anwender erschrecken oder amüsieren soll. Sie geben etwa vor, wie ein Virus oder dessen Payload zu agieren, in Wirklichkeit richten sie aber keinen Schaden an. Ferner können sie auch Hardwarefehlermeldungen vorgeben oder Nachrichten über angeblich auf dem Rechner gefundene Viren ausgeben.

Diese Programme können sich nicht selbst replizieren (in dem Falle würde so ein Programm unter die Definition des Virus fallen).

Würmer

Würmer sind Programme, die sich ausbreiten, indem sie sich selbst über Netze kopieren. Sie befallen dabei das Netz als Gesamtheit und nicht isolierte Rechner.

Sie sind dabei, anders als Viren, nicht an ein Wirtsprogramm gebunden und bewegen sich selbständig von Rechner zu Rechner, indem sie in den Speicher eines Rechners eindringen, dort weitere Netzwerkadressen von anderen Computern ermitteln und Kopien ihrer selbst dorthin schicken.

Die besondere Gefährlichkeit liegt in ihrer hohen Ausbreitungsgeschwindigkeit. So können sie sich, bevor sie bemerkt werden, bereits auf zahlreiche andere Rechner kopiert haben.

MIRC-Würmer

Bei den MIRC-Würmern handelt es sich um konkrete Fälle von aufgetretenen Würmern:

Der Internet Relay Chat (IRC) ist ein System, mit dem über das Internet durch das rasche Austauschen von Text-Nachrichten von User zu User eine schriftliche Kommunikation in Echtzeit möglich ist (Sogenannte „Chats“ oder Konferenz-Verbindungen). Über direkte Client-zu-Client-Verbindungen (DCC) können auch Dateien ausgetauscht werden.

MIRC ist ein verbreiteter IRC-Client für Windows und unterstützt eine Skript-Sprache, die vom MIRC-Programm benutzt wird. Solche Skripte können als Dateien von Nutzer zu Nutzer verschickt werden.

Diese Skriptsprache wurde auch zur Schaffung von Würmern mißbraucht.

Mailer / Mass Mailer

Dies sind die zur Zeit sehr verbreiteten Würmer, die sich per E-Mail von PC zu PC versenden. Sie werden durch Ausführung eines entsprechenden Attachments oder ohne Zutun des Benutzers durch in eine E-Mail eingebettete Skripte (z. B. JavaScript) aktiviert. LoveLetter oder MTX gehören zu den Würmern dieser Art.

Hostile Agents

Bei Hostile Agents (also etwa „feindseligen Agenten“) handelt es sich um eine vergleichsweise neue Art der Malware, die ihre Bedrohung mit dem Wachsen des Internets entfaltet.

Die Technik der Agents (Applets und Controls) wurde mit der Absicht eingeführt, um das Design von Multi-Media-Web-Seiten zu ermöglichen. Dabei wurde auf geringere zu übertragende Datenmengen Wert gelegt: Elemente wie Animationen oder Laufschriften werden nicht erzeugt, indem ganze Bilder-Sequenzen übertragen werden, sondern es werden Bilder durch die Applets lokal errechnet, unter Umständen unter Verwendung nachträglich übertragener, aktueller Daten. Die Applets enthalten also Instruktionen zum Aufbau der zu übertragenen Web-Seite an das empfangende System.

„Hostile“ wird ein Applet genannt, das Handlungen ausführt, die nicht im Sinne des Benutzers liegen oder das den Benutzer dazu bringt, diese auszuführen.

Solche Handlungen können das Ausspähen (d.h. das Auslesen und Versenden) von persönlichen oder geheimen Daten wie Paßwörtern, Seriennummern oder PINs für das Online-Banking sein oder alle Arten schädigenden Verhaltens wie etwas das Löschen oder Verändern von Daten (Formatieren der Festplatte) oder das Installieren von Viren auf dem Rechner beinhalten.

Die Tatsache, daß der Internet Explorer 4.0 von Microsoft über VBScript-Routinen verfügt, über die auf das Dateisystem des PCs zugegriffen werden kann, stellt eine neue Verwundbarkeit von solchen Systemen gegenüber feindlicher Software aus dem Internet dar.

VBScript ist eine Erweiterung zur Gestaltung aktiver Internet-Seiten und dient zusätzlich als Spracherweiterung für Windows 98. Sie ist der Ersatz für die Batch-Sprache.

Bei der Installation des Internet Explorers zusammen mit Windows 98 ist im Brower per default die mittlere Sicherheitsstufe eingestellt, so daß eine Web-Seite auf diesen PC zugreifen und aktiv werden kann. Dies wird von Microsoft nicht als Fehler, sondern als erweiterte Funktionalität (Feature statt Bug) angesehen.

JAVA - Applets

Mit Java-Applets werden Applets bezeichnet, die in der Programmiersprache JAVA der Firma SUN geschrieben wurden. Auf den anbietenden Web-Servern liegt der JAVA-Code der Applets in bereits kompilierter Form vor.

Diese Applets werden vom Browser heruntergeladen und lokal auf dem Rechner des Clienten ausgeführt. Die Ausführung erfolgt in einer „virtuellen Maschine" des Browsers, die den rechnerunabhängigen Code des Applets auf dem individuellen Rechnersystem zum Laufen bringt. Dieser Vorgang läuft innerhalb eines sogenannten „Sandkastens" ab. Dies ist ein besonderer, nach außen abgeschotteter Bereich, der die Aktionen des Java-Applets beschränkt. So darf nach diesem Modell ein Applet nicht von einer Festplatte lesen oder darauf schreiben.

Weitere Sicherheitsmaßnahmen sind der „Bytecode Verifier", der den Java-Code auf unerlaubte Befehle überprüft, und zum anderen gibt es noch den „Class Loader", mit dem der Java-Code an Manipulationen des Sandkastens gehindert wird.
Diese Menge von Einschränkungen unterbindet eine große Anzahl von potentiell gefährlichen, aber auch evtl. nützlichen Handlungen. Dennoch verbleiben viele unerwünschte Dinge, die mit Java erreicht werden können, wie z.B. „Denial of service" - Angriffe oder das Senden gefälschter E-Mails.

Auch wenn dieses Modell immerhin ein gewisses Maß an Sicherheit bietet, sind doch auch Sicherheitslücken aufgetreten, die durch Programmierfehler entstandenen sind und durch Schwachstellen im Konzept der Sprache, die sich daraus ergeben, daß das Java-Sicherheitsmodell nicht schon ein Bestandteil bei der Entwicklung der Programmiersprache war, sondern erst im nachhinein hinzugefügt wurde.

Bekanntgewordene Bugs werden in der Regel in neueren Versionen der Browser behoben, aber ebenso häufig und schnell werden neue Sicherheitslücken entdeckt. Es bleibt das Risiko, daß auch Java-Applets außerhalb des Sandkastens handeln können.

Das hier beschriebene Prinzip gilt nur für Java-Applets, aber nicht für eigenständige, in Java geschriebene Applikationen. Diese (vom Internet unabhängigen) Anwendungen sind mit den gleichen Möglichkeiten versehen wie in anderen Programmiersprachen geschriebene Programme.

Speziell signierte Java-Applets dürfen den Anwender um erweiterte Rechte bitten. Werden ihnen diese erteilt, können sie den schützenden Sandkasten verlassen.

JAVA Script

Diese Erweiterung des HTML-Standards durch die Firma Netscape erlaubt eine Steuerung des Internet-Browsers. Anweisungen dieser Programmiersprache werden in den HTML-Code eingebunden und können auch Java-Applets aufrufen. Java Script wurde für die Nutzung im Internet entwickelt und sieht darum keine Zugriffe auf das Dateisystem des Rechners vor, ebenso keine Funktionen, um Verbindungen zu anderen Rechnern aufzubauen.
Dennoch sind auch Zugriffe auf sicherheitsrelevante Bereiche des Computers mit Java Script möglich. So konnte E-Mail unbeaufsichtigt versendet werden. Um diese Möglichkeit einzudämmen, haben neuere Versionen der Browser eine zusätzliche Abfrage eingebaut.

Wenn der Trend dazu führen sollte, höhere Rechte für Java-Script-Programme vorzusehen, die ein Zertifikat vorweisen können, ergibt sich die gleiche Problematik, wie im Abschnitt über die Active X-Controls beschrieben.

ActiveX - Controls

Der Internet Explorer der Firma Microsoft unterstützt ab der Version 3.0 aus dem Jahr 1996 die Software „ActiveX", mit der Microsoft seinen eigenen Ansatz entwickelt hat, der es Erstellern und Anbietern von World-Wide-Web-Seiten ermöglichen soll, die unterschiedlichsten Komponenten direkt in HTML-Seiten einzubetten.

Dazu werden (relativ) kleine, aber ansonsten vollwertige Programme, die sogenannten Controls, automatisch von den Web-Seiten der

Anbieter auf den Rechner des Netzsurfers übertragen und dort installiert. Auf diese Weise werden dem Browser zusätzliche Funktionen hinzugefügt.

Diese Controls können in vielen verschiedenen Programmiersprachen erstellt werden, neben C/C++ oder DELPHI z.B. auch JAVA.

Der Netscape Navigator bringt nicht von sich aus eine Unterstützung für Active-X mit, kann aber mit einem Plug-in („ScriptActive"-von Ncompass Labs) um diese Funktionalität erweitert werden.

Es ist im Gegensatz zu JAVA bei ActiveX kein Sicherheitsmodell vorhanden und es nicht mit internen Vorschriften geregelt, was ein Control darf oder nicht darf.

Die Active-X-Controls haben von vornherein Zugriff auf Rechnerressourcen wie die Festplatte und dürfen auch Netzwerkverbindungen, zu anderen Internet-Rechnern aufbauen.

Mit der Mächtigkeit der Funktionen ergibt sich eine entsprechend große Bandbreite möglicher Attacken.

Im Bewußtsein, daß diese Technik inhärent unsicher ist, hat der Hersteller dem Benutzer die Möglichkeit gegeben, zwischen drei verschiedenen Schutzgraden (niedrig, mittel, hoch) zu wählen. Wählt der Benutzer nun den maximalen Schutzgrad, werden nur noch Controls angenommen, die eine Zertifizierung aufweisen können.

Eine solche Zertifizierung, die vor dem eigentlichen Download angibt, wer das entsprechende Active-X-Control programmiert hat, kann aber bestenfalls verhindern, daß das Programm auf seinem Weg durchs Internet verfälscht wird, sie schützt aber nicht davor, daß ein Control von vornherein böswillig programmiert wird. Sie enthält auch keinerlei Aussagen über die korrekte Funktionaltität des Controls und dient damit weniger der Sicherheit des Benutzers als der Sicherheit des Programmierers des Controls vor der unlizensierten Weitergabe des Controls.

Cookies

Mit dem Prinzip der Cookies soll das mehrmalige Aufsuchen der gleichen Internet-Adresse beschleunigt und vereinfacht werden, indem vom Benutzer spezifische, in der Regel von ihm selbst eingegebene Informationen auf seinem eigenen Computersystem gespeichert werden, um bei einer späteren Session erneut darauf zurückgreifen zu können, ohne etwa eine Kundennummer erneut eingeben zu müssen. Zudem kann die Webseite angepaßt werden und ein persönliches, auf den einzelnen Nutzer zugeschnittenes Aussehen haben.

Ein einzelner Server kann höchstens 20 Cookies auf einem lokalen Rechner hinterlassen, jeder davon maximal 4 KB groß. In seiner Struktur besteht ein Cookie aus einem Namen, einem Wert (ein String) und einem URL-Pfad, wobei der Wert alles sein kann, was der Webserver selbständig ermitteln kann oder der Nutzer von sich aus preisgibt, etwa durch das Ausfüllen eines Online-Formulars.

Wenn ein Cookie eine Identifikationsnummer enthält, kann der Anbieter in einer eigenen Datenbank dort zuvor gespeicherte Daten über den Nutzer wiederfinden und zuordnen. Um jedoch einem Cookie eine personelle Identität zuzuordnen, muß der Nutzer erst auf irgendeiner Seite seine Personalien preisgeben, wenn dieses nicht schon durch das Auswerten von Logdateien gelingt.

Diese Informationen werden als reiner Text im Hauptspeicher oder auch auf der Festplatte gespeichert (persistente Cookies). Da dieser Text kein ausführbarer Code ist, ist es für einen Cookie nicht möglich, selbst unerwünschte Handlungen auszuführen.

Um doch noch möglichst viele Informationen über das Surf-Verhalten der Nutzer zu erhalten, wird von einigen werbetreibenden Firmen folgender Trick versucht:
Durch das Plazieren von Werbe-Banners auf möglichst vielen Seiten erhalten sie eine Beteiligung an all diesen Seiten und erwerben damit das Recht, Cookies zu erstellen und auszulesen. Weil die Banner auch Links zu der eigenen Seite darstellen, können Cookies darüber verschickt werden. Diese Cookies stammen dann nicht von der eigentlich gerade geladenen Seite, sondern von dem Werbeunternehmen.

Angesichts der Vielzahl von Web-Seiten kann so eine Firma jedoch für ein wirkliches Bewegungsprofil viel zu wenige Seiten überblicken.

Welche Schäden können Computerviren / Malware verursachen?

Der Schaden reicht von einfachen Bildschirmmeldungen bis zur Zerstörung aller Programme und Daten auf allen beschreibbaren Datenträgern. Einige Viren überschreiben das BIOS (CIH-Virus), oder aktivieren BIOS-Paßwörter, sofern das BIOS nicht mit einem entsprechenden Schreibschutz versehen ist. Einige Trojaner spähen auch die Paßwörter aus oder suchen in Texten nach interessanten Schlüsselwörter und übertragen diese dann an eine vorgegebene Adresse. Auch die Fernsteuerung befallener PC ist möglich. Es gilt: Was sich programmieren und als Schadensfunktion nutzen läßt, wird früher oder später auch genutzt werden!

Wie werden Viren / Malware übertragen?

Malware / Viren können auf allen Datenträgern (z.B. CD, MO, ZIP, JAZ oder Bänder) enthalten sein. Sogar mit Original-Software wurde bereits Malware und speziell Viren verbreitet. Der Hauptübertragungsweg ist heutzutage allerdings die E-Mail.

Eine Übertragung kann ebenfalls über Netzwerke stattfinden. Dabei sind die verwendeten Übertragungsdienste, wie z. B. WWW, FTP, E-Mail, News usw., nur das Transportmedium.

Wie schütze ich mich vor Computerviren / Malware?

- Machen Sie regelmäßig Backups.
- Schalten Sie das Booten von Diskette im BIOS ab.
- Installieren Sie einen Virenscanner und sorgen Sie für regelmäßige Updates.
- Prüfen Sie jede neue Datei/Diskette oder anderen Datenträger und jeden E-Mail-Anhang auf Viren, am besten mit einem automatisch laufenden (sog. On-Access-) Hintergrund-Virenscanner.
- Öffnen Sie nur E-Mail-Anhänge, die Sie erwarten.
- Wenn das Betriebssystem über die Möglichkeit von Zugriffsbeschränkungen verfügt, nutzen Sie diese auch. Alle Programme, die der Benutzer nicht ändern darf, sollten schreibgeschützt sein. Dann kann auch ein vom Benutzer gestarteter Virus diese Datei nicht verändern. Nicht ausreichend ist das Read-Only Attribut von DOS. Dieses Attribut kann von jedem Programm übergangen werden.
- Deaktivieren Sie Java/JavaScript/VBScript und ActiveX im Betriebssystem, im Web-Browser und im E-Mail-Programm.
- Deaktivieren Sie automatische Update-Funktionen
- Deaktivieren Sie Cookies

Erstellen Sie eine Notfall-Bootdiskette mit allen benötigten Treibern und einem Virenscanner. Für den Notfall müssen Sie in der Lage sein, den Rechner unabhängig von allen möglicherweise infizierten Programmen auf der Festplatte booten zu können und einen Virenscanner zu starten bzw. das Backup wieder einzuspielen. Denken Sie auch daran, den Virenscanner und dessen Signaturen aktuell zu halten.

Wie lassen sich Computerviren / Malware entdecken?

Nicht alles, was aussieht wie ein Virus, muß auch gleich einer sein. Es können auch Software-/Hardwaredefekte oder Unverträglichkeiten vorliegen.

Als Hinweise für eine Infektion können dienen:
- Rechner liest beim Start kurz von der Festplatte und bleibt dann hängen (evtl. Bootsektorvirus?)
- Dateilängen haben sich verändert
- Programme haben ihr Verhalten verändert, stürzen ab.
- Dauernde Festplattenaktivität, obwohl kein Programm gestartet ist
- Dateien werden als verändert gemeldet, obwohl sie nicht editiert wurden.
- In Texten (z.B. Word-Dokumenten) werden Worte hinzugefügt, Wörter vertauscht oder am Ende werden Kommentare angehängt.

Einige Viren geben auch Bildschirmmeldungen aus, spielen eine Melodie, vertauschen Buchstaben auf der Tastatur oder manipulieren die Bildschirmausgabe.

Viele Viren benutzen Tarnmechanismen oder spezielle Techniken, um ihre Weiterverbreitung zu sichern:

Stealth-Technik: Wenn der Virus im Speicher aktiv ist, entfernt der Virus sich beim Laden des infizierten Programmes aus diesem und verhindert so seine Entdeckung.

Polymorphie: Der Virus verschlüsselt oder verändert sich selbst. Dazu fügt er in sein Programm weitere, völlig nutzlose Befehle ein oder vertauscht einige seiner Programminstruktionen. Z. B. tauscht er a + b in b + a aus. Die Berechnung liefert das selbe Ergebnis, der Programmtext sieht aber anders aus.

Fast Infector: Der Virus infiziert sofort möglichst viele Dateien. Da diese Methode sehr aggressiv vorgeht, kann die Infektion oft durch sehr starke Festplattenaktivität bemerkt werden.

Slow Infector: Diese Virenart geht sehr langsam vor, Dateien werden nur dann infiziert, wenn auf sie schreibend zugegriffen wird. Dieser Virus kann auch längere Zeit inaktiv sein.

Ich habe einen Virus, was nun?

Grundregel: KEINE PANIK!

Unüberlegte Aktionen können den Schaden beträchtlich vergrößern.

In den meisten Fällen ist es am sinnvollsten, alle Programme zu beenden und den Rechner abzuschalten. Danach starten Sie den Rechner von einer virenfreien Bootdiskette und starten danach, ebenfalls von Diskette, eventuell auch von CD, einen Antivirenscanner. Wichtig dabei ist, daß kein möglicherweise infiziertes Programm von der Festplatte Ihres Rechners gestartet werden darf! Sonst ist der Virus im Speicher aktiv und verhindert seine Entfernung.

Infizierte Programme sollten eigentlich gelöscht werden und von der Originaldiskette/CD neu installiert werden. Ein Reparieren der Datei kann nicht generell empfohlen werden, da sich nur die wenigsten Viren spurlos entfernen lassen. Das reparierte Programm mag zwar anscheinend laufen, jedoch könnte der Virenrest im Programm ein Störfaktor sein, der ein unvorhersagbares Verhalten auslösen kann.

Bei Makroviren kann das Dokument repariert werden. Zur Vorsicht sollten dabei alle im Dokument enthaltenen Makros entfernt werden. Eigene Makros müssen nach der Entfernung wieder eingespielt werden.

Überprüfen Sie auch alle Disketten, CDs und Backups auf eine Infektion.

Fragen Sie im Zweifelsfalle einen Experten für Virenbekämpfung!

Impressum
Universität Hamburg
Fachbereich Informatik
Virus-Test-Center
Vogt-Kölln-Straße 30
22527 Hamburg

Telefon: ☎040 / 42883 - 2234 (Labor)
☎040 / 42883 - 2405 (Sekretariat)

Fax: ☎040 / 42883 - 2226

Web-Seite: http://agn-www.informatik.uni-hamburg.de

Spenden an das Virus-Test-Center bitte an die
Landeshauptkasse Hamburg, Kto-Nr. 101 600
Hamburgische Landesbank, BLZ 200 500 00
Stichwort: 34013 Prof. Brunnstein / FB Informatik