



2 MALWARE

2.1 Definition und Funktionsweise

Als Malware bezeichnet man Computerprogramme, die unerwünschte, meist auch schädliche Aktionen ausführen.

2.1.1 Den Begriff Malware verstehen

Oft wird „Computervirus“ irrtümlich (leider auch von Fachleuten) als Synonym von Malware verwendet, was darauf zurückzuführen ist, dass Viren die ersten Schadprogramme waren, die die Computerleistung beeinträchtigten. In der Zwischenzeit sind Schädlinge mit ganz unterschiedlichen Arbeitsweisen entwickelt worden, sodass eine genaue Differenzierung dieser Programme notwendig wurde. Als Sammelbegriff hat sich das Kunstwort *Malware*, zusammengesetzt aus **malicious** (böartig) und **Software** etabliert.

Bezeichnung	Wirkung
Virus	Ein einfacher Virus wird durch Aufruf des Programmes, in dem er sich eingenistet hat, aktiv. Er verbreitet sich durch Aktivierung der infizierten Datei auch auf andere Dateien und innerhalb des Netzwerkes. Je nachdem, wo der Virus wirkt, unterscheidet man Computer-, Datei-, System-, Makro- und Bootviren.
Wurm	Die Wirkung entspricht dem eines einfachen Virus. Er verbreitet sich allerdings automatisch, beispielsweise über das Adressmaterial für E-Mails. Dazu nutzt er die Sicherheitslücken des Betriebssystems.
Trojaner	Programme, die als nützliche Anwendung in das Computersystem eingeschleust werden, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllen, meist zum Schaden des Anwenders. Mit solchen Programmen kann der <i>Hacker</i> Passwörter oder Tastatureingaben herausfinden, um damit einen Zugang in den Computer, aber auch auf Bankkonten des Anwenders erlangen. Je nach Infektionsfunktion werden differenzierte Begriffe verwendet: Backdoor-Trojaner, PWS-Trojaner, Trojan-Downloader ...
Hoax	Wörtlich Scherz oder Falschmeldung; meistens erfolgt eine derartige Scherz- oder Falschmeldung mittels E-Mail. Sie gibt bekannt, dass ein Virus unterwegs sei, und fordert den Anwender auf, eine bestimmte Aktion auszuführen. Ein Hoax soll meist nur erschrecken.



Bezeichnung	Wirkung
DoS-Attacken	Denial of Service (DoS)-Attacken, die im Internet zur Beeinträchtigung von Webservices führen; zB kann es durch die Versendung einer Vielzahl von E-Mails oder durch Bombardierung von Anfragen zur Überlastung von Servern kommen. Dadurch können andere Aktionen nicht mehr hinreichend ausgeführt werden. Die Server sind durch Überlastung nicht mehr erreichbar.
Spyware	Durch Spy (spionieren) wird das Online-Verhalten von Webnutzern beim Surfen ausspioniert und dieses Wissen an andere weiter gegeben. Aus den Ergebnissen, die in der Regel in Tabellen gespeichert und über E-Mails an den Urheber gesendet werden, können Rückschlüsse auf das Konsumverhalten gezogen und die Werbewirksamkeit durch gezielten Einsatz von abgestimmten Methoden gesteigert werden.

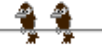
2.1.2 Verschiedene Möglichkeiten zum Verbergen von Malware kennen, wie: Rootkit, Backdoor-Trojaner

Rootkit

Ein Rootkit ist eine Software, die im Hintergrund versucht, einen Fremdzugriff zu ermöglichen und vertrauenswürdige Daten weiterzusenden. Der Name kommt von Root (engl. für Wurzel; Administratorebene) in dem es installiert wird, um damit zukünftige Logins eines Eindringlings zu verbergen und Prozesse und Dateien zu verstecken. Diese Programme verstecken Malware so gut im System, dass selbst viele Virens Scanner sie nicht mehr finden.

Backdoor-Trojaner

Es sind die gefährlichsten und häufigsten Trojaner. Mit einem Backdoor-Trojaner kann der Urheber oder „Master“ des Trojaners mit Hilfe von Fernadministration den Opferrechner angreifen. Im Gegensatz zu den legitimen Fernadministrationsprogrammen können Sie den Backdoor-Trojaner nicht erkennen. Dadurch werden ohne Ihr Wissen Programme installiert, gestartet und genutzt. Wenn Backdoor-Trojaner einmal installiert sind, können sie Dateien verschicken, empfangen, ausführen oder löschen, sie können vertrauliche Daten aus dem Computer entnehmen oder Computeraktivitäten protokollieren.



2.2 Typen

2.2.1 Typen von sich selbst verbreitender Malware kennen und ihre Funktionsweise verstehen, wie: Virus, Wurm

Ein Virus ist ein Programm, das andere Programme „infizieren“ kann. Dabei kann dieses Programm so verändert werden, dass dieses eine möglicherweise mutierte Kopie von dem Programm enthält. Infiziert bedeutet, dass sich der Virus in die Befehlskette des ursprünglichen Programms (Wirtsprogramm) einschleust, so dass der Versuch, ein legitimes Programm auszuführen, auch gleich zur Ausführung des Virus führt.

Ein Wurm ist ein Programm, das sich selbst kopiert und verbreitet, ohne sich an ein Wirtsprogramm anzuhängen. Ein Wurm wandert über Netzwerkverbindungen von einer Maschine zur nächsten. Die „Absicht“ der Würmer ist es, so viele Computer wie möglich innerhalb eines Netzwerks zu befallen. Würmer vermehren sich durch kopieren und brauchen keine weiteren Befehle, um sich innerhalb eines Firmennetzwerks oder über das Internet zu verbreiten.

2.2.2 Malware kennen für Datendiebstahl, Betrug oder Erpressung und die Funktionsweise dieser Malware verstehen, wie: Adware, Spyware, Botnet, Keylogger und Dialer

Adware

Adware ist eine werbeunterstützende Software, mit der Werbebanner automatisch eingeblendet, abgespielt oder auch Downloads gestartet werden. Adware-Programme werden oft in Freeware- oder Shareware-Programme eingebaut, wo sie sich dann indirekt über die Nutzung des Werbebanners gegenfinanzieren.

Durch das Einblenden von Werbung wird das Lesen der Webseiten beeinträchtigt. Zudem hat Adware häufig einen Code, mit dem persönliche Informationen der Nutzer ohne deren Kenntnis ausspioniert werden.

Spyware

Diese Art von heimtückischer Software wird vor allem beim Downloaden eines vermeintlich kostenlosen Angebots auf Ihrem Computer installiert. Dort können die Surfgewohnheiten festgehalten werden oder die Eingabe von Passwörtern und Kontonummern ausspioniert werden. Auch Angaben über die benutzte Software, von heruntergeladenen Dateien oder die Konfiguration der Hardware sind für den Eindringlich wertvolle Informationen.



Botnet

Ein **Botnet** oder **Botnetz** ist eine Gruppe von Bots¹. Die Bots laufen auf vernetzten Rechnern und nutzen die Ressourcen des lokalen Rechners ebenso wie die Verbindung zu den im Netz verfügbaren Computern.

Man unterscheidet „gutartige“ Bots und „böartige“ Bots. Letztere werden beispielsweise zum Sammeln von E-Mail-Adressen für Werbezwecke, für das massenhafte unautorisierte Kopieren von Webinhalten bis hin zum systematischen Ausspionieren von Softwarelücken von Servern mit dem Ziel des Einbruchs in diese Server eingesetzt.

Keylogger

Als Keylogger bezeichnet man Hard- oder Software zur Aufzeichnung von Tastatureingaben. Das Ziel dieser Methode ist, alle Aktivitäten am Computer zu kontrollieren. So kann auch ein unerlaubter Zugriff auf Daten nachvollzogen werden, welche E-Mails geschrieben wurden oder auf welche Internetseiten von diesem Computer zugegriffen wurde.

Der Nachteil aber ist, dass diese Aufzeichnungen auch unbemerkt an einen Angreifer übermittelt werden können und so eine immense Gefahr darstellen. Der Angreifer kann dann aus diesen Informationen für ihn wichtige Daten, wie zB Anmeldeinformationen oder Kreditkartennummern filtern.

Einen Schutz vor dem Zugriff eines Hardware-Keyloggers bietet die Verwendung einer virtuellen Tastatur (Bildschirmtastatur). Gegen Software-Keylogger hilft nur die Verwendung von Anti-Spyware-Programmen und Virens Scanner.

Dialer

Mit so genannten Dialer-Programmen (Einwahlprogramme) kann eine Verbindung über das Telefonnetz hergestellt werden. Wird diese Methode jedoch dazu verwendet, auf eine kostenintensive Mehrwertnummer umgeleitet zu werden, so entstehen für den Geschädigten enorme Telefonrechnungen. Ein solches Programm muss in der Regel heruntergeladen, d.h. angeklickt und am Computer gespeichert, und anschließend ausgeführt werden. Dialer gibt es oft auf Webseiten mit erotischem Inhalt oder auch auf Seiten, die andere Services (denkbar sind zB Seiten für Klingeltöne oder Logos, Hausaufgaben, Referate) anbieten.

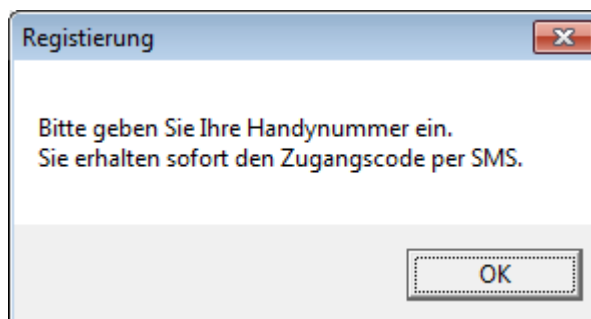
Um sich zu schützen, kann man bei seiner Telefongesellschaft eine Sperrung aller 0939- Nummern (in Deutschland 0190 bzw. 0900-9) für den eigenen Anschluss beantragen.

¹ Unter einem **Bot** versteht man ein Programm, das selbstständig Aufgaben abarbeitet, ohne dabei auf eine Interaktion mit einem menschlichen Benutzer angewiesen zu sein.



Benutzer, die sich ausschließlich über DSL² mit dem Internet verbinden, sind nicht von Dialern betroffen. Dafür besteht die Gefahr, über das Mobilfunknetz auf eine Mehrwertnummer verbunden zu werden.

Beachten Sie daher nebenstehende Aufforderung, die Ihnen bei Besuch einer Website zur Eingabe einer Handynummer erscheint und meiden Sie die Aktivierung.



2.3 Schutz

Schutz vor dem Eindringen von Malware und vor deren Aktivierung am Computer bieten Antivirusprogramme. Diese durchforsten (scannen) Programmcodes, erkennen dabei Viren und beseitigen diese.

2.3.1 Die Funktionsweise und die Grenzen von Antiviren-Software verstehen

Ein Virenschanner oder Antivirusprogramm ist eine spezielle Software, die bekannte Computerviren, Computerwürmer und Trojanische Pferde aufspüren, blockieren und auch löschen kann.

Um die schädliche Software zu erkennen, besitzt jeder Virenschanner eine Datenbank mit ihm bekannter Viren und anderer schädlicher Software. Gefundene Programmcodes, werden mit den Einträgen der Datenbank verglichen. Wenn eine Datei oder ein Teil einer Datei mit einem Beispiel aus dieser Datenbank übereinstimmt, leitet der Virenschanner Neutralisierungsmaßnahmen ein, um die infizierte Datei zu beseitigen oder zu säubern.

Wie arbeiten Virenschanner?

Die meisten Programme bieten 2 Methoden der Virensuche.

- **On Access** Ein Hintergrundüberwachungsprogramm (Guard) überprüft laufend alle Dateien, die vom System gelesen, geschrieben oder bearbeitet werden.
- **On Demand** Durch den User wird der Scan manuell gestartet. Danach werden Dateien, Ordnern oder Datenträgern gezielt durchsucht.

² **Digital Subscriber Line.** Übertragungsstandards bei der Daten mit hohen Übertragungsraten über einfache Kupferleitungen gesendet und empfangen werden können; im privaten Bereich meist ADSL.



2.3.2 Laufwerke, Ordner und Dateien mit Antiviren-Software scannen; Scans mit Antiviren-Software planen

Auf jedem Computer sollte ein Antivirus-Programm installiert sein. Für den privaten Gebrauch werden auch verschiedene kostenlose Programme angeboten. Bei manchen Programmen kann eine zeitlich begrenzte Testinstallation vorgenommen werden.

Planen Sie in welchen Zeitabständen ein kompletter Virusscan stattfinden soll. Das könnte auch bei jedem Neustart des Computers erfolgen. Natürlich dauert das eine Weile und daher kann es sinnvoll sein, einzelne Laufwerke oder externe Datenträger nur von Zeit zu Zeit komplett zu scannen. Ordner, in denen Programme abgelegt sind, sollten öfters überprüft werden. In jedem Fall sollten bei einem Download von Dateien oder beim Abrufen Ihrer E-Mails diese Dateien immer einem Virusscan unterzogen werden.

In einem Netzwerk sind die Server meist so konfiguriert, dass On-Demand-Virencans außerhalb der Geschäftszeiten durchgeführt werden. Damit können zeitraubende Unterbrechungen ausgeschlossen werden.

2.3.3 Den Begriff Quarantäne verstehen und die Auswirkung der Quarantäne auf infizierte oder verdächtige Dateien kennen

Wenn ein Virens Scanner schädliche Dateien findet, gibt er in den meisten Fällen eine Warnung an den User weiter, mit der Frage, was jetzt geschehen soll. Die Möglichkeiten reichen von Auslagern der befallenen Datei in einen Quarantäne-Bereich³ über einen Reparaturversuch bis zum endgültigen Löschen der infizierten Datei.

Wann Quarantäne – Wann Löschen

Wo liegt nun der Unterschied zwischen Quarantäne und Löschen? Die Option mit Quarantäne ist bei falschen Virus-Meldungen sinnvoll.

In Quarantäne gehören Dateien, bei denen nicht genau bekannt ist, ob diese wirklich „infiziert“ sind und ob man diese Datei für den Betrieb des Computers nicht doch braucht. Es wäre es zB fatal, wenn das Antivirus-Programm ein kritisches Programm wie Explorer.exe falsch markiert und daraufhin die Datei sofort gelöscht werden würde. In diesem Fall ist das Verschieben der markierten Datei in die Quarantäne die bessere Entscheidung. Dort ist die gefundene Datei vom Rest des Computers abgeschottet und kann keinen Scha-

³ Quarantäne ist ein Ordner, der im Antivirus-Programmordner angelegt wird. In diesem werden infizierte Dateien verschoben und können solange das Antivirusprogramm aktiv ist, keinen Schaden anrichten.



den anrichten. Ist jedoch die Funktionalität des Computers nicht mehr gegeben, so kann die Datei wieder aus der Quarantäne zurückgeholt werden. Treten jedoch keinerlei Probleme auf, kann die Datei aus der Quarantäne unwiderruflich gelöscht werden.

2.3.4 Verstehen, weshalb es wichtig ist, Software-Updates zu installieren und Virensignaturen zu aktualisieren

Ständig tauchen neue Viren und Würmer auf. Daher wird die Datenbank mit den Virussignaturen⁴ auch ständig aktualisiert. Fast alle Anbieter von Antivirusprogrammen bieten automatische Aktualisierungen (Updates) an. Nutzen Sie dieses Angebot. Es liegt in Ihrem Interesse, dass Sie immer gegen die aktuell bekannten Viren gewappnet sind.

⁴ Virussignatur: Erkennungsmuster eines Virus, das zur Identifikation verwendet wird.

