Malware – Malicious Software
Böswillige Software

1. Virus

Ein Computervirus (Singular; das, umgangssprachlich auch der Computervirus) ist ein sich selbst vermehrendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich damit reproduziert. Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion.

Der Begriff Computervirus wird auch fälschlich für Computerwürmer und Trojanische Pferde genutzt, da der Übergang inzwischen fließend und für Anwender oft nicht zu erkennen ist.

Ein Virus verbreitet sich, indem es sich selbst in noch nicht infizierte Dateien kopiert und diese ggf. so anpasst, dass das Virus mit ausgeführt wird, wenn das Wirtsprogramm gestartet wird. Zu den infizierbaren Dateien zählen normale Programmdateien (exe, com, sys,…), Programmbibliotheken (dll), Skripte (bat), Dokumente mit Makros (VBA, Excel, …) oder anderen ausführbaren Inhalten sowie Bootsektoren (auch wenn Letztere normalerweise vom Betriebssystem nicht als Datei repräsentiert werden).

Die Verbreitung auf neue Systeme erfolgt durch versehentliches (gelegentlich auch absichtliches) Kopieren einer infizierten Wirtsdatei auf das neue System durch einen Anwender. Dabei ist es unerheblich, auf welchem Weg diese Wirtsdatei kopiert wird: Früher waren die Hauptverbreitungswege Wechselmedien wie Disketten, heute sind es Rechnernetze (z.B. via E-Mail zugesandt, von FTP-Servern, Web-Servern oder aus Tauschbörsen heruntergeladen). Es existieren auch Viren, die Dateien in freigegebenen Ordnern in LAN-Netzwerken infizieren, wenn sie entsprechende Rechte besitzen.

Achillesferse eines Virus

Damit ein Virenscanner ein Virus identifizieren kann, benötigt er dessen Signatur. Ein Virus versucht, ein System zu infizieren, und dies geschieht z. B. bei einem Linkvirus durch das Anhängen an ein bestehendes Programm. Dabei muss es (abgesehen von überschreibenden Viren) zuerst prüfen, ob es dieses Programm bereits infiziert hat – sprich, es muss in der Lage sein, sich selbst zu erkennen. Würde es dies nicht machen, könnte es ein Programm theoretisch beliebig oft infizieren, was aufgrund der Dateigröße und der CPU-Belastung sehr schnell auffallen würde. Dieses Erkennungsmuster – die Signatur – kann unter gewissen Umständen auch von Virenscannern genutzt werden, um das Virus zu erkennen. *Polymorphe* Viren sind in der Lage, mit verschiedenen Signaturen zu arbeiten, die sich verändern können, jedoch stets einer Regel gehorchen. Daher ist es den Herstellern von Anti-Viren-Software relativ einfach und schnell möglich, ein neues Virus nach dessen Bekanntwerden zu identifizieren.

2. Wurm

Im Gegensatz zu Viren warten Würmer nicht passiv darauf, von einem Anwender auf einem neuen System verbreitet zu werden, sondern versuchen aktiv in neue Systeme einzudringen. Sie nutzen dazu Sicherheitsprobleme auf dem Zielsystem aus, wie z.B.:

a. Netzwerk-Dienste, die Standardpasswörter oder gar kein Passwort benutzen
b. Design- und Programmierfehler in Netzwerk-Diensten
c. Design- und Programmierfehler in Anwenderprogrammen, die Netzwerkdienste benutzen (z.B. E-Mail-Clients)

Hauptaufgabe des Wurms ist die eigene Verbreitung unter Ausnutzung bekannter Systemfehler.

Die Würmer selbst können u.U. durch laufend aktualisierte Antiviern-Programme erkannt werden. Die Tätigkeit eines Wurms kann durch Netzwerk-Sicherheitsmaßnahmen (Paketfilter, Personal Firewall eingeschränkt werden.

3. **Trojaner**, (korrekt: Trojanisches Pferd)

Als Trojanisches Pferd bezeichnet man ein Programm, welches als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine ganz andere Funktion erfüllt.

Die heimliche Funktion eines Trojaners kann darin bestehen, ein Schadprogramm auf dem PC zu installieren, welches infolgedessen unabhängig vom Trojaner meist versteckt auf dem PC arbeitet. Der tatsächliche Nutzen einer Datei, die ein Trojanisches Pferd enthält, kann beliebiger Art sein. So können u.a. eigenständige Spionageprogramme auf den Rechner gelangen (z. B. Sniffer oder Komponenten, die Tastatureingaben aufzeichnen, so genannte Keylogger). Auch ermöglicht ein solcher Trojaner die heimliche Installation eines Backdoorprogramms, welches es gestattet, den Computer über ein Netzwerk (z.B. dem Internet) fernzusteuern, ohne dass der Anwender dies kontrollieren kann. Durch das Löschen des Trojanerprogramms werden die heimlich installierten Schadprogramme nicht automatisch mit entfernt.

4. Hoax

Ein Hoax (engl., Jux, Scherz, Schwindel) bezeichnet im Deutschen eine Falschmeldung, die sich per E-Mail, Instant Messenger oder auf anderen Wegen (SMS, MMS, ...) verbreitet, von vielen für wahr gehalten und daher an viele Freunde weitergeleitet wird.

Auch Kettenbriefe, die per E-Mail weitergeleitet werden, können zu den Hoaxes gezählt werden, denn hier existiert selten ein realer Hintergrund, der die Verbreitung rechtfertigen würde.

5. Dialer

Dialer (deutsch: Einwahlprogramme) sind im engeren Sinne Computerprogramme, mit deren Hilfe über das analoge Telefon- oder das ISDN-Netz eine Verbindung zum Internet oder anderen Computernetzwerken aufgebaut werden kann. So ist bei vielen Betriebssystemen bereits ein Standard-Einwahlprogramm für Verbindungen nach dem Point-to-Point Protocol (PPP) mitgeliefert. Bei Windows nennt es sich „DFÜ-Netzwerk“. Das Einwahlprogramm muss gestartet werden, wenn man eine Internet-Verbindung aufbauen möchte, und so lange laufen, bis man die Verbindung nicht mehr benötigt und diese schließt.

Heute denkt man jedoch beim Begriff „Dialer“ gewöhnlich an solche Dialer, die von unseriösen, teilweise sogar kriminellen Anbietern verbreitet werden, um ohne ausdrückliche oder nur unzureichende Zustimmung des Kunden von diesem erhöhte Gebühren abzurechnen.

6. SPAM

Spam ist der unverlangte, massenhafte, meist strafbare Versand von Nachrichten. Diesen Missbrauch bezeichnet man als Spamming/Spammen und die Täter als Spammer.

Eine Haftungsfrage für den Versand von E-Mail-Würmern und Trojanern, die den größten Anteil ausmachen dürften, ist in Deutschland noch umstritten. Unter sehr eingeschränkten Bedingungen sehen einige Autoren zumindest Unternehmen als haftbar an, für Privatpersonen verneint die Literatur überwiegend eine Haftungsverpflichtung.

Strafrechtlich ist das Erstellen und Verbreiten von Würmern, Viren und Trojanern als Computersabotage relevant. 2005 wurde in Deutschland deswegen ein Schüler als Autor von Netsky und Sasser zu einem Jahr und neun Monaten Haft auf Bewährung verurteilt.

7. SCAM

Der englische Ausdruck Scam (dt. Betrug, Beschiss) hat sich im deutschsprachigen Raum als Eigenname für den Betrug mittels Massen-E-Mails etabliert. Die Empfänger werden unter Vorspiegelung falscher Tatsachen (vgl. Social Engineering) dazu gebracht, an Schneeballsystemen teilzunehmen oder in Erwartung zugesagter Vermittlungsprovisionen gegenüber den Absendern (den *Scammern*) finanziell in Vorleistung zu treten.

8. Phishing

Phishing ist eine Form des Trickbetruges im Internet. Die Bezeichnung „Phishing“ leitet sich vom Fischen (engl. fishing) nach persönlichen Daten ab.

Der Phisher schickt seinem Opfer offiziell wirkende Schreiben, meist E-Mails, die es verleiten sollen, vertrauliche Informationen, vor allem Benutzernamen und Passwörter oder PIN und TAN von Online-Banking-Zugängen, im guten Glauben dem Täter preiszugeben.

9. Pharming

Pharming ist eine Manipulation der Hostdatei von Webbrowsern, um Anfragen auf gefälschte Webseiten umzuleiten. Es ist eine Fortentwicklung des klassischen Phishings.

Der Begriff "Pharming" rührt von dem Umstand her, dass die Pharming-Betrüger eigene große Server-Farmen unterhalten, auf denen gefälschte Webseiten abgelegt sind.

Pharming hat sich als Oberbegriff für verschiedene Arten von DNS-Angriffen etabliert. Eine Methode dabei ist die lokale Manipulation der Host-Datei. Dabei wird unter Zuhilfenahme eines Trojaners oder eines Virus eine gezielte Manipulation des Systems vorgenommen mit der Konsequenz, dass von diesem System nur noch gefälschte Websites abrufbar sind, selbst wenn die Adresse korrekt eingegeben wurde

10. Spoofing

Spoofing (engl. für "Manipulation", "Verschleierung") nennt man verschiedene Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität.

Früher stand Spoofing ausschließlich für den Versuch des Angreifers, Pakete so zu fälschen, dass sie die Absenderadresse eines anderen (manchmal vertrauenswürdigen) Hosts tragen. Heutzutage umfasst Spoofing alle Methoden, mit denen sich Authentifizierungs- und Identifikationsverfahren untergraben lassen, die auf der Verwendung vertrauenswürdiger Adressen oder Hostnamen beruhen.

Im Einzelnen unterscheidet man:

- ARP-Spoofing: Dient der Umleitung von Datenpaketen auf der MAC-Ebene.
- DNS-Spoofing: Zum Umleiten von URL/DNS-Informationen. → Pharming
- IP-Spoofing: Versenden von Nachrichten unter einer gefälschten IP-Absenderdresse
- Mail-Spoofing: Mails mit falscher Absenderadresse. (Ausnutzung der SMTP-Schwäche)
- URL-Spoofing: Anzeige einer falschen, anstelle der richtigen Web-Seite. → Pharming

11. DoS = Denial of Service

Als DoS-Angriff (dt. etwa „Dienstverweigerungsangriff“) bezeichnet man einen Angriff auf einen Host (Server) mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht dies durch Überlastung. Erfolgt der koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von einem **DDoS** (Distributed Denial of Service). Normalerweise werden solche Angriffe nicht per Hand, sondern mit Backdoor-Programmen oder Ähnlichem durchgeführt, welche sich von alleine auf anderen Rechnern im Netzwerk verbreiten und dadurch dem Angreifer weitere Wirte zum Ausführen seiner Angriffe bringen

Schutzmaßnahmen

Der erste Schritt zur Vermeidung von Gefahren in vernetzten Systemen besteht darin, das System auf bekannte Schwächen zu untersuchen, eine *Fehleranalyse* zu erstellen. Anschließend versucht man eine oder mehrere der nachfolgend dargestellten Maßnahmen zu implementieren:

- Software (Betriebssystem und Anwendungssoftware) immer aktuell halten, Updates regelmäßig installieren.
- Aufpassen beim Umgang mit E-Mails. Anhänge nur dann öffnen, wenn Absender und Rechtmäßigkeit der E-Mail zweifelfrei feststehen.
- Ein aktuelles und regelmäßig aktualisiertes Antivirenprogramm verwenden.
- Einsatz einer Firewall (nicht gegen Viren)
- Identifizerungs- und Authentifizierungsvorschriften (Benutzernamen, Passwörter, Codekarten)
- Regeln zur Vergabe von Passwörter (mind. 8 Zeichen, Groß-/Kleinschreibung, Sonderzeichen)
- Festlegung der Zugangsrechte zu bestimmten Unternehmensbereichen und zu bestimmten Softwaregruppen, Einschränkung der Administrationsrechten.
  Bsp. Als reiner Benutzer/Anwender unter Windows niemals mit vollen Administrationsrechten arbeiten, sondern als *eingeschränkter Benutzer*.
- Festlegung von Regeln und Rechten für den Fernzugang (Homeoffice, Aussendienstmitarbeiter, Fernwartung)
- Festlegung von Regeln für die Wartung des Systems und das Einspielen von Patches/Updates
- Festlegung von Maßnahmen für den Angriffsfall

(Quellen: Wikipedia → Computervirus (1), Computervirus (1), (2),)