Nur für den internen Gebrauch

1. Malware (Übersicht)

Als Schadprogramm (engl. *malware*: Kunstwort aus *malicious* - "böswillig" - und *software*) bezeichnet man Computerprogramme, die eine offene oder verdeckte Schadfunktion aufweisen und mit dem Ziel entwickelt werden, Schaden anzurichten. Schadfunktionen können zum Beispiel die Manipulation oder das Löschen von Dateien oder die Kompromittierung der Sicherheitseinrichtungen (wie z.B. Firewalls und Antivirenprogramme) eines Computers sein.

Mit Schadprogramm ist nicht ein fehlerhaftes Programm gemeint, auch wenn es durch den Fehler Schaden anrichten kann. Vielmehr geht es um die mutwillige Zerstörung.

Es existieren folgende Typen von Schadprogrammen:

- Computerviren sind die ältesten Programme dieser Art; sie verbreiten sich, indem sie Kopien von sich selbst in Programme, Dokumente oder Datenträger schreiben.
- Ein Computerwurm ähnelt einem Computervirus, verbreitet sich aber direkt über Netzwerke wie das Internet und versucht in andere Computer einzudringen.
- Ein Trojanisches Pferd ist eine Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogrammes mit einem versteckt arbeitenden, bösartigen Teil, oft Spyware oder eine Backdoor. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.
- Eine Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang („Hintertür“) zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft für Denial-of-Service-Angriffe benutzt.
- Als Spyware bezeichnet man Programme, die Informationen über die Tätigkeiten des Benutzers sammeln und an Dritte weiterleiten. Ihre Verbreitung erfolgt meist durch Trojaner.

Oft werden auch Dialer (Einwahlprogramme auf Telefon-Mehrwertrufnummern) zur Malware gezählt, obwohl sie nicht grundsätzlich dazu zählen. Illegale Dialer-Programme allerdings führen die Einwahl heimlich – unbemerkt vom Benutzer – durch und fügen dem Opfer (oft erheblichen) finanziellen Schaden zu (Telefonrechnung).*Siehe auch:* Computersicherheit, Rootkit, Antivirenprogramm, Pharming, Phishing, Firewall, Adware, Keylogger, Spam

2. **Bezahlsysteme im ONLINE-Handel** (Quelle:SZ vom 19.02.08)

www.paypal.de
www.ukash.de
www.giropay.de
www.cliklandbuy.de
www.eprepaid.de

Achtung! Es gibt ähnlich klingende Pishing-Seiten, z.B.:
www.ukash-auction.uk.com

3. Regeln für ein sicheres System Quelle:PC-Welt 03/08, S.82

Beachten Sie bitte: Ich kann hier nur Hinweise aus der genannten Quelle und anderen Ratschlägen und Erfahrungen notieren, die mir persönlich bedeutsam erscheinen. Wichtig wäre es, die Quelle selbst ausführlich zu lesen.

1. Aktualisieren Sie Ihr System regelmäßig
   Update-Archiv anlegen (Falls Neuinstallation erforderlich)
2. Aktualisieren Sie Software zuverlässig
   Nur erforderliche Software installieren, alles andere deinstallieren. Software auf den neuesten Stand halten
3. Setzen Sie eine Router-Firewall ein
   Viele Router verfügen standardmäßig über eine vorkonfigurierte Firewall.
4. Arbeiten und surfen Sie als eingeschränkter Nutzer
5. Öffnen Sie keine Mailanhänge von unbekannten Absendern
   - Im Zweifelsfall: Vor dem Öffnen telefonisch nachfragen.
   - Vorsicht: Dateiendungen spiegeln nicht mit Sicherheit den erwarteten Dateityp wider. (rechnung.PDF<zeilenumbruch>.PIF ist als PDF sichtbar, in Wirklichkeit aber als PIFausführbar und häufig schädlich)
   - Auch JPG Dateien müssen nicht unbedingt Bilder sein.
   - Auch JAR Archive werden mißbraucht
6. Lassen Sie sich beim Surfen nicht täuschen
   - Typosquatting: Vertippen bei Eingabe einer URL führt recht häufig zu einer ähnlich klingenden präparierten Seite.
   - Es gibt päparierte WEB 2.0 Seiten, bei denen ein versehentlicher Klick auf das Hintergrundbild zu einem Malware-Server führt. >> Adresszeile beobachten!
   - Vertrauliche Informationen nur in Formularen mit verschlüsselter Verbindung eingeben. In der Adresszeile muss https:// stehen.
   - Vorsicht, wenn Zertifizierungsnachfragen gestellt werden.
   - Ausdrücke in der Adresszeile können sehr unübersichtlich sein: **http://hans:geheim@www.example.org:80/demo/example.cgi?land=de&stadt=aa#abschnitt1**

   Vergeben Sie stets *verschiedene* sichere Kennwörter
   (Auch für alle Benutzerkonten)
7. Empfangen Sie Mails nur als Plain-Text (Klartext...direkte Zeichencodierung)
   - Links können maskiert sein
   - Keine HTML-Formulare ausfüllen
8. Installieren Sie keine Tools aus unbekannten Quellen
   - Gefahr: Zum Installieren sind Administratorrechte erforderlich!
   - Wenn gut bekannt: Herstellerseite zum Download benutzen, sonst z.B. seriöse PC-Zeitschriften
10. Nutzen Sie immer NTFS-Rechte
    - Ein eingeschränktes Benutzerkonto hat keine Schreibrechte im Windows-Ordner, damit können Systemdateien nicht manipuliert werden.
    - Sie können auch NTFS-Rechte nutzen um eigene Dateien zu schützen.