Bedrohungen für Ihren PC

Beginn: 13:00 Uhr

und Ihren Geldbeutel !

Wie gelangt Schad-software auf den PC ?

Es gibt viele Wege, wie ein Programm auch auf Ihren Rechner gelangen kann:

1. Der Anwender lädt das Programm herunter und installiert es im guten Glauben. (z.B.: Dialer)

2. Das Programm wird mittels Spam-Mail als Anhang verschickt.
   Der Anwender installiert es aus Neugier / im guten Glauben.

3. Eine infiziertes Bild / Datei / Email wird geöffnet und die Maleware gelangt auf den PC.

4. Die Maleware ist auf einer CD / DVD, einem USB-Stick, einer Diskette oder einer HDD versteckt und installiert sich per Autostart.

5. Das Programm installiert sich durch Ausnutzen von Sicherheitslücken selbst.

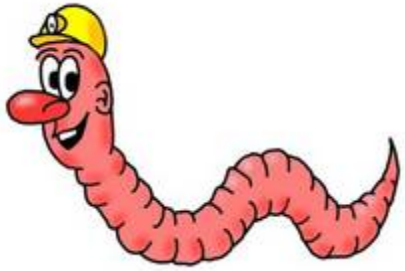
Alle Betriebssysteme sind betroffen !

- **2005** wurde das erste Virus für Handys geschrieben.
- **20.3.2009** Auf mehreren Terrabyte schlummern **etwa 20 Millionen Computerviren**, schätzt Marx, der das größte Virentestlabor Deutschlands leitet.
- **Täglich kommen 25.000 bis 35.000 neue Viren hinzu**
- **12 Millionen Viren waren es allein im Jahr 2008.**

Trojanische Pferde

- **… sind Programme, die als nützliche Programme getarnt, weitere unbekannte Funktionen installieren.**
- **Diese Funktionen laufen eigenständig auf dem PC und lassen sich nicht mit dem Trojanerprogramm beenden oder gar löschen.**
- **So können z.B.: Viren / Spyware / Bots, … auf den PC gelangen.**

Trojanische Pferde



- … können auf jedem Weg auf den PC gelangen, mit dem Daten auf den Computer gebracht werden.
- über Datenträger, Netzwerkverbindungen, Internet, Tauschbörsen, präparierte Webseiten, E-Mails.
- Die Verbreitung erfolgt dann durch den Anwender des PCs selbst. Wahrscheinlichkeit, dass der Anwender das Programm an weitere Anwender weitergibt.
- Für die Verbreitung per E-Mails wird meistens ein Computerwurm verwendet, der das Trojanische Pferd transportiert und installiert.
- Moderne Trojaner sind von Virenscannern nur noch schwer erkennbar.

Ein Computervirus …

- … ist ein sich selbst verbreitendes Programm, welches sich in andere Programme einschleust und sich damit reproduziert.

- Einmal gestartet, kann es vom Anwender nicht kontrollierbare Veränderungen am Status der Hardware (zum Beispiel Netzwerkverbindungen), am Betriebssystem oder an der Software vornehmen (Schadfunktion).

- Computerviren beeinträchtigen die Computersicherheit

Computerviren können…

- **Veränderungen am Status der Hardware vornehmen.**
- **Veränderungen am Betriebssystem vornehmen.**
- **Veränderungen an Programmen vornehmen.**
- **Veränderungen an Schutzprogrammen vornehmen.**

- **die Computersicherheit beeinträchtigen.**
- **das Betriebssystem zerstören.**
- **vorhandene Programme zerstören.**
- **zu Systemabstürzen führen.**

- **sich verändern / verstecken / verkleiden**
- **sich weiterverbreiten.**
- **Ihnen hohen Kosten verursachen.**

Ein Computerwurm

- ist ein Programm, das sich über Netzwerke verbreitet und dafür kein Wirtsprogramm benötigt.

- Es verbreitet sich zum Beispiel durch das Versenden infizierter E-Mails (selbstständig oder durch ein E-Mail-Programm), durch IRC-, Peer-to-Peer- und Instant-Messaging-MMS.

- Ein Wurm muss nicht unbedingt eine Schadensroutine enthalten. Da das Wurmprogramm aber auf den infizierten Systemen sowie auch auf den zu infizierenden Systemen, Ressourcen zur Weiterverbreitung bindet, kann es bereits dadurch erhebliche wirtschaftliche Schäden anrichten.

- Des Weiteren können Würmer die Belastung anderer Systeme im Netzwerk wie Mailserver, Router und Firewalls erhöhen.

Als Spyware …

- **…wird üblicherweise Software bezeichnet, die Daten eines PC-User ohne dessen Wissen oder Zustimmung an den Hersteller der Software oder an Dritte sendet oder dazu genutzt wird, dem Benutzer direkt Produkte anzubieten.**

Ein PC könnte infiziert sein, wenn eines oder mehrere der folgenden Symptome auftreten:

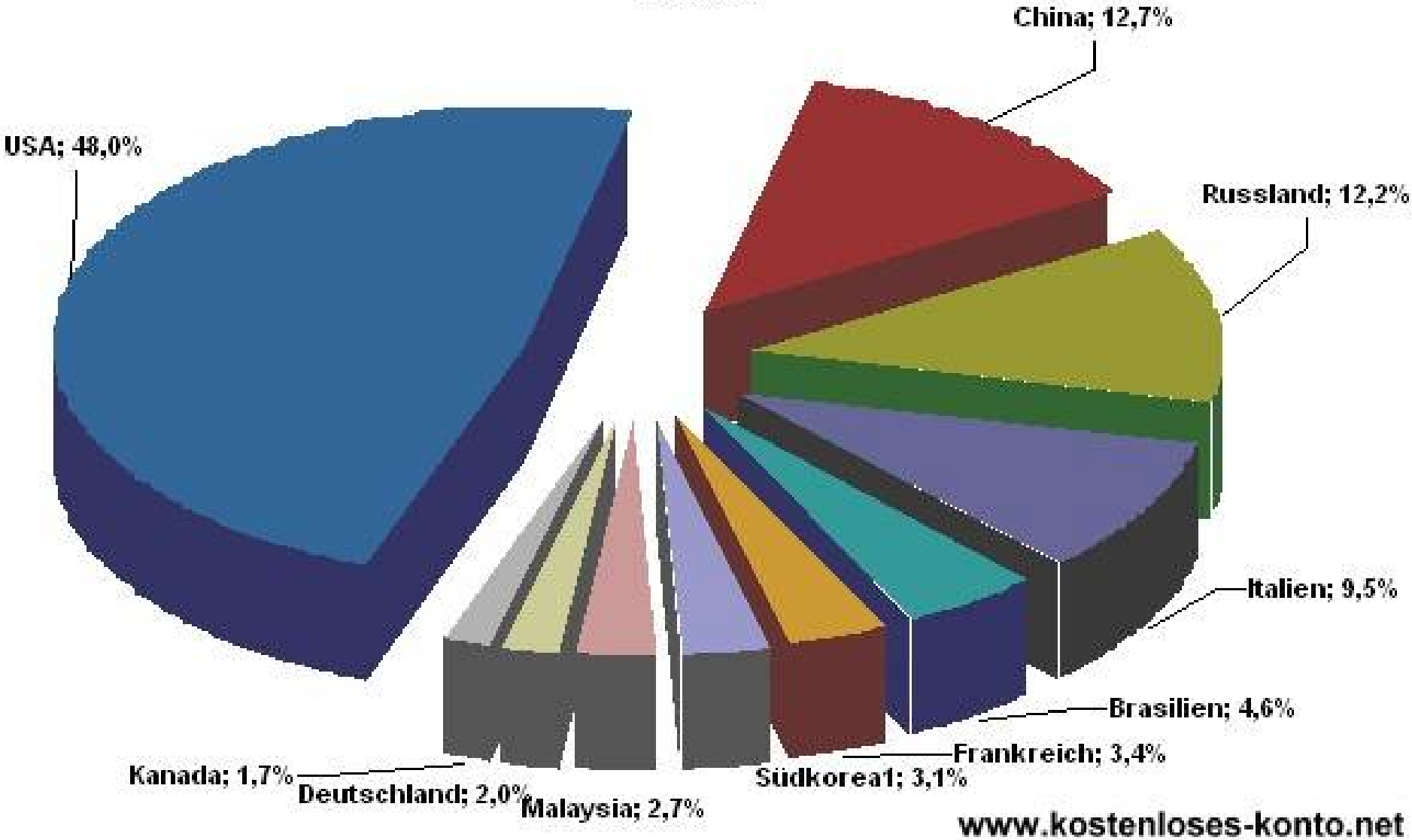
- **Der PC ist extrem langsam, besonders beim Surfen im Internet.**
- **Der Internet-Explorer öffnet Werbefenster, die in keinem erkennbaren Zusammenhang zu den besuchten Websites stehen.**
- **Die Browser-Startseite wurde geändert.**
- **Im Favoritenordner stehen Links, die nicht vom Benutzer gespeichert wurden.**
- **Der PC verbindet sich selbständig mit dem Internet.**
- **Die Firewall meldet laufend Versuche von Programmen, die eine Verbindung zum Internet herstellen wollen.**
- **Selbständiges Löschen**
- **Es befindet sich eine Spyware-Warnung am Desktop als Hintergrund, die zum Beispiel den Erwerb eines angeblichen Anti-Spyware-Programms bewirbt**

Phishing

Phishing werden Versuche genannt, über gefälschte WWW-Adressen an die Daten eines Internet-Benutzers zu gelangen.

Passwort f**ishing** = **Phishing** = Passwort angeln

In diesen 10 Ländern wurden die meisten Phishing-Seiten bzw. Phishing-Trojaner installiert.



www.kostenloses-konto.net

Neue Methoden

- **Aktuell gelingt es Phishing-Betrügern vor allem mit Hilfe von Trojanern und anderer Schadware, sich in dem Kommunikationsweg zwischen Bankkunde und Bank zuschalten und Daten abzugreifen, die dann bei der Bank nie ankommen.**
- **Diese moderne Form des Abgreifens von Kontozugangsdaten ermöglichte es den Tätern, auch vergleichsweise moderne Systeme wie das e-TAN-Verfahren zu überlisten.**

Phishing Ziele

- **Phishingziele sind dabei Zugangsdaten für: z. B. Onlinebanking, PayPal, Versandhäuser, Internet-Auktionshäuser, webbasierende Onlineberatungen oder Singlebörsen.**
- **Mit den gestohlenen Zugangsdaten kann der Urheber der Phishing-Attacke die Identität seines Opfers übernehmen (Identitätsdiebstahl) und in dessen Namen Handlungen ausführen.**
- **Durch den Missbrauch der persönlichen Daten entstehen beträchtliche Schäden in Form von**
  - **Vermögensschäden (Überweisung von fremden Konten)**
  - **Rufschädigung (Versteigerung gestohlener Waren unter fremdem Namen)**
  - **Schäden durch Aufwendungen für Aufklärung & Wiedergutmachung.**

SPAM

- **Als Spam oder Junk (englisch für ‚Abfall‘ oder ‚Plunder‘) werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden und häufig werbenden Inhalt haben.**

Schäden durch Spam

- Allein in den USA entsteht pro Jahr ein Schaden von 22 Milliarden US-Dollar.
- 100.000.000.000 (100Milliarden) Std. Arbeitszeit zum Sichten und Löschen der Spam-Mails.
- Demnach macht Spam mittlerweile 97 % des gesamten E-Mail-Volumens aus.

Maßnahmen gegen Spam

z.B.

Mozilla Thunderbird Spamfilter
MS-Outlook / Outlook Express Junkflter
Windows Mail

Was sind Dialer?

Dialer sind Programme die in der Regel dazu dienen, gebührenpflichtige Sonderrufnummern (01805, 0190, 0900, … anzuwählen um Kosten über die Telefonrechnung des Anrufers abzurechnen.

Das kann sowohl legal als aber auch illegal sein.

Legal oder illegal ?

Legale Dialer

- Beim Besuch einer Website wird der Download des Dialers angeboten.
- Der Anbieter weist verständlich auf die Kosten der Verbindung hin.
- Der Dialer installiert sich nicht automatisch.
- Der Dialer installiert sich nicht als Standardverbindung.
- Der Anwender entscheidet, ob er sich über den Dialer einwählen will.
- Vor und während der Verbindung werden die Kosten angezeigt.
- Der Dialer kann vollständig deinstalliert werden.

Betrügerische Dialer

- Beim Besuch einer Website wird ein automatischer Download gestartet.
- Es erfolgen keine oder unklare Angaben über den Tarif der Verbindung.
- Der Dialer installiert sich automatisch.
- Der Dialer installiert sich als Standardverbindung.
- Die Einwahl über die Verbindung des Dialers erfolgt ohne Rückfrage automatisch.
- Die Kosten werden nicht angezeigt.
- Der Dialer lässt sich nicht/umständlich deinstallieren.

Keine Gefahr für Kabelmodem oder DSL-Modemrouter

- **Dialer funktionieren nur bei direkter Einwahl ("dial-up"), also bei Verbindungen über ein analoges- bzw. ein ISDN- oder ADSL-Modem.**
- **Wer einen ständigen Zugang ("DSL") hat, etwa durch ein Kabelmodem oder einen Router, ist vor Dialer-Attacken sicher.**
- **Wenn am PC allerdings ein *zweiter Zugang* - etwa fürs Faxen - besteht, kann dieser sehr wohl von einem Dialer missbraucht werden.**