

Viren, Würmer und anderes Ungeziefer

Über bösartige Programme im Allgemeinen und auf
dem Mac im Speziellen

Begriffe

- Viren “infizieren” Programme und verbreiten sich, wenn das Programm weitergegeben und ausgeführt wird
- Würmer verbreiten sich, einmal gestartet, selbst
- Trojaner warten im Hintergrund auf Aktivierung

Die Typen lassen sich jedoch nicht immer eindeutig abgrenzen, zumal es auch Mischformen gibt.

Viren

- “Klassische” Viren hängen sich an Programme an
- Bootsektor / Autostart-Viren
- Makroviren (Word-Dateien), “Melissa”

Internet

Das Verbreitungsmedium Nr. 1



“Berühmte” Schädlinge

- Brain (erster PC-Virus), 1986
- Sendmail-Wurm (E-Mail), 1990
- Michelangelo (Virus), 1992
- Melissa (Makro-Virus), März 1999
- I love you (E-Mail-Attachment), Mai 2000
- Kournikova (E-Mail-Attachment), Feb. 2001
- Code Red und Nimda (Webserver), August / September 2001

... Fortsetzung

- SQL-Slammer (MS-SQL-Server), Januar 2003
- W32.Blaster (RPC), August 2003
- Sober, Bagle/Beagle, Netsky, ...

Methoden

- zumeist: E-Mail-Attachment
- gelegentlich: Lücken in Services (IIS, RPC, SQL-Server)
- auch: Tauschbörsen
- das Hauptproblem jedoch ...

... bist Du!



- “Social Engineering”
- Sorglosigkeit
- Sicherheitsupdates
- Virenschanner / -filter

Virenautoren

Wer schreibt eigentlich Viren und warum?



Motivation

- Früher: “Spaß” / Schadenfreude (Fun-Viren)
- Früher: Vandalismus (Daten löschen)
- Heute: “Armee von Bots” für Attacken (DDoS)
- Heute: Spambots
- Heute: Daten ausspionieren (Keylogger)

Und auf dem Mac?

Welche - theoretischen und
realen - Gefahren existieren für
Mac-User?



AppleScript

```
tell application "Mail"
  set newMessage to make new outgoing message with
    properties { subject:"some witty subject",
                content:"some random garbage",
                sender:"some@loser.tld" }
  tell newMessage
    make new to recipient at end of to recipients
with properties { name:"Victim",
                  address:"victim@other.tld" }

    send
  end tell
end tell
```

Fehler in Programmen

- Aktuell z.B. Buffer-Overflow in JavaScript in Safari
- Sicherheitsprobleme im Unix-Unterbau
- Unsichere Voreinstellungen

Solche Probleme sind zwar auf einem Unix-System schwierig(er) auszunutzen, können aber z.B. genutzt werden, um Programme zum Absturz zu bringen.

Zusammenfassung

- Sicherheitsupdates einspielen!
- Virens Scanner sind derzeit auf dem Mac Geldverschwendung
- Virenfilter machen schon eher Sinn.
- Sich informieren, News-Sites lesen (z.B. Heise)
- Vor allem aber: Hirn einschalten!