

Wurmfreier Apfel

Die steigende Popularität von Apple-Rechnern macht Mac OS immer mehr zum lohnenden Ziel für Cyber-Kriminelle. Zeit, sich Gedanken über einen Virenschutz zu machen.

Mac-User zelebrieren gerne den Mythos, Viren könnten einem Apple-Rechner nichts anhaben. Dabei wurde bereits einer der ersten Computer-Viren – der vom 15-jährigen Richard Skrenta entwickelte „Elk Cloner“ aus dem Jahr 1982 – auf einem Apple II programmiert. Auch aktuell sitzen die Apple-Jünger nicht im Elfenbeinturm: Die Zahl der Viren und Trojaner für das Apple-Betriebssystem nimmt stetig zu. Eine nicht zu unterschätzende Gefahr geht auch von den so genannten Zero-Day-Attacken aus: Über solche Schwachstellen im Betriebssystem, für die noch kein Security-Patch existiert, können Hacker in den Rechner eindringen.

Den Millionen Schadprogrammen für Windows stehen bisher nur einige Hundert für das Mac-Betriebssystem gegenüber. Das liegt zum einen daran, dass Apple seinen Computern bereits zahlreiche technische Schutzvorkehrungen von Haus aus mit auf den Weg gibt. Eine "Sandboxing" genannte Technik schließt unbekannte Programme in einen streng getrennten Bereich ein. Die Programme können auf keine Dateien außerhalb der Sandbox zugreifen und keine anderen Programme und Prozesse starten. Weitere Sicherheitsfunktionen sind die "Library Randomization", mit der verhindert wird, dass Schadprogramme wichtige Systembibliotheken finden, sowie "Execute Disable", eine Technik, die den Arbeitsspeicher des Mac schützt. Dazu kommen noch automatische Updates, ein Anti-Phishing-Filter im Safari-Browser, eine eingebaute Verschlüsselung und Assistenten für sichere Passwörter.

Der zweite Grund ist eine schlichte Kosten-/Nutzen-Rechnung. Cyberkriminelle konzentrieren sich auf die am weitesten verbreiteten Computersysteme – bis heute vor allem Microsoft Windows. Doch mit der zunehmenden Beliebtheit von Apple-Notebooks wird auch Mac OS für Hacker immer interessanter. Nach Zahlen von w3counter.com hatte das Mac-Betriebssystem im August 2009 bereits einen Marktanteil von etwas mehr als sieben Prozent erreicht. Virenanalysten gehen davon aus, dass die kritische Grenze für die Rentabilität bei etwa zehn Prozent liegt. Erreicht ein Computersystem diesen Anteil am

Markt, werden die kriminellen Aktivitäten deutlich lohnender und nehmen stark zu. Den Trend dazu kann man schon seit Anfang 2009 erkennen. Da zeigte der Trojaner Mac.iServices, der infizierte PCs ins Bot-Netz iBotnet eingliederte, sein hässliches Haupt. Er wurde über eine infizierte Raubkopie von iWork 09, einer Bürosoftware von Apple, verteilt. Nach Analystenangaben waren bis zu 20.000 Anwender betroffen, die sich das Kuckucksei mittels Bittorrent-Download auf den Computer gezogen hatten. Kurz darauf ging es in ähnlicher Weise mit einer Raubkopie von Photoshop CS4 weiter, auch hier war ein Familienmitglied aus der Reihe Trojan.iServices in das Programmpaket eingebaut.

Grundschutz statt Panikmache

Dennoch: Im Vergleich zur Windows-Welt sind solche Ausbreitungswellen Kleinkram. Reichen ein paar Hundert Schadprogramme, um eine Anti-Crimeware-Lösung auf dem Mac zu rechtfertigen? Apple ist definitiv dieser Meinung und empfiehlt den Einsatz von zusätzlicher Sicherheitssoftware (www.apple.com/macosx/security).

Kaspersky Lab bietet Sicherheitslösungen aus einer Hand für Windows, Linux – und auch einen speziell auf Mac-Rechner abgestimmten Schutz. Kaspersky Anti-Virus for Mac (www.kaspersky.de/anti-virus_for_mac) ergänzt die in Mac OS integrierten Sicherheitsmechanismen optimal. Die Software überprüft Dateien und E-Mail-Anhänge in Echtzeit – sowohl beim Öffnen, Download als auch Speichern. Infizierte Objekte können gelöscht oder in die Quarantäne verschoben werden. Dateien in Quarantäne versucht Kaspersky Anti-Virus for Mac zu desinfizieren und wiederherzustellen. Wichtig: Dank des Datei-Backups gehen keinerlei Daten verloren.

Auch wenn Mac-Computer für die meisten Arten von Malware nicht anfällig sind, so sind sie ein effektiver Weg, Viren zu verbreiten. Cyberkriminelle nutzen ungeschützte Macs als Einfallstor in private und Firmennetzwerke und als Verbreitungsplattform innerhalb "sozialer Netzwerke". Vom Mac-Benutzer unbemerkt werden so klassische Bedrohungen wie Viren, Trojaner, Würmer, Spyware und Adware zu PCs von Freunden oder Kollegen weitergeleitet. Kaspersky Anti-Virus for Mac erkennt und blockiert neben den für Mac OS gefährlichen

Schädlingen auch Malware für Windows und Linux. So wird eine Weitergabe eventueller Probleme an Freunde und Kollegen vermieden.

Das Schutzpaket ist ganz klar als Ergänzung gedacht, auch dann, wenn man auf einem Mac zwei Betriebssysteme benutzt. Durch aktuelle Virtualisierungsprogramme lässt sich ein Windows XP oder Vista innerhalb von Mac OS X installieren und gleichzeitig benutzen. Durch Verfahren wie "Seamless Mode" ist nicht einmal ein Unterschied zu merken, wenn ein Windows-Programm auf dem Apple Desktop läuft. Aber gerade dann ist es wichtig, beide Systeme vor Schadsoftware zu schützen.

Die Benutzeroberfläche von Kaspersky Anti-Virus for Mac entspricht dem gewohnten Mac-Style und ist sowohl für Einsteiger als auch für fortgeschrittene Nutzer konzipiert. Berichte über den Schutzstatus sowie weitere wichtige Informationen über aktuelle Anwendungsaktivitäten sind grafisch einfach aufbereitet. Dabei arbeitet die Software sehr Ressourcen-schonend: Steigt die Anwenderaktivität, ordnet sich der Scanner unter und beeinträchtigt somit die Leistung der gerade ausgeführten Anwendungen nicht. Trotz hoher Scanleistung hat Kaspersky Anti-Virus for Mac mit nur 1%iger CPU-Auslastung keinen merklichen Einfluss auf die Systemperformance.

Fazit: Auch Macs sind nicht sicher vor Angriffen und bedürfen daher zusätzlicher Schutzmaßnahmen – egal ob zu Hause oder im Büro.