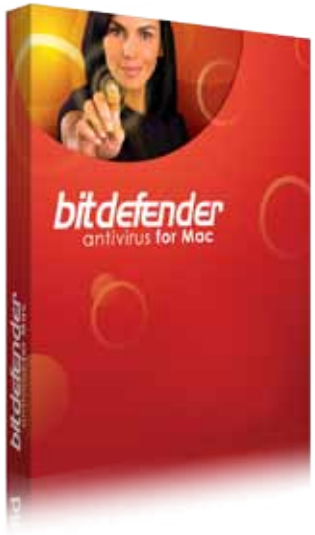
# bitdefender ANTIVIRUS FÜR MAC®




Seit der Einführung moderner Computertechnologie sind digitale Bedrohungen, sogenannte E-Threats, sprichwörtlich an Apple-Anwendern vorbeigegangen: Von einigen wenigen Ausnahmen einmal abgesehen, haben Viren, Würmer und Trojaner auf Apple-Rechnern nie wirklich Schaden angerichtet. Doch mit dieser scheinbaren Sicherheit in der heilen Welt des Apfels ist es mittlerweile vorbei. Virenprogrammierer und Malware-Autoren konzentrieren ihre Bemühungen zunehmend auch auf die Suche nach Sicherheitslücken im Mac OS und den beliebtesten Mac-Applikationen.

## Mac OS X – Malware-Historie

Anfang der achtziger Jahre, genauer gesagt 1981, gewannen Apple II-Systeme zunehmend an Beliebtheit, sowohl bei Privatanwendern als auch bei Akademikern. Bereits ein Jahr später machte sich der damals 15-jährige Schüler Rich Skentra die große Popularität der Apple II-Serie zu Nutze und programmierte das Elk Cloner-Virus – das erste bekannte Virus überhaupt. Elk Cloner verbreitete sich selbständig über infizierte Floppydisks, welche seinerzeit das gebräuchlichste Medium zur Aufbewahrung, Transport und Weitergabe von Daten waren. Aus heutiger Sicht mutet diese Art von Schädlingen, die kleine Bildchen oder lustige Texte auf den Monitor zauberten, bzw. wie im Fall von Elk Cloner ein Gedicht, wie ein harmloser Scherz an. Wie auch immer, weitere Apple-Viren mit den Namen Virus 1, Virus 2 und Virus 3 folgten schon sehr bald nach.

Die zunehmende Verbreitung von Mac-Systemen führte im Laufe der Zeit zu neuen, aggressiveren Viren, deren Abwehr zunehmend schwieriger wurde. Anfang 2006 erschien eine gänzlich neue Art von Bedrohungen für Mac-Betriebssysteme: OSX/Leap-A, auch OSX/Oompa-A genannt, wurde speziell für Mac OS X maßgeschneidert. Mit seinen Wurm-Fähigkeiten verbreitete er sich selbständig via iChat: Er tarnte sich als Bilddatei, die angeblich einen Screenshot des brandneuen Apple-Betriebssystems beinhalten sollte.

## Zeitgemäße Abwehr

Stand 2010 hat sich Apples Mac OS X zur Version 10.6 weiterentwickelt – und Apple hat mittlerweile weltweit einen Marktanteil von 9 Prozent erreicht. Hochgerechnet auf mehr als 1 Milliarde Personal Computer eine stattliche Zahl von potenziellen Opfern – das haben auch Cyberkriminelle längst erkannt und arbeiten an neuen Strategien und Methoden, die direkt auf Apple-Anwender zielen.

In diesem Augenblick kursieren mehr als 270 verschiedene E-Threats, die ausnahmslos für das Mac OS X entwickelt wurden. Und genauso wie in der Windows-Welt sieht sich der durchschnittliche Mac-Anwender mit einer Vielzahl unterschiedlicher Risiken konfrontiert: So wird beispielsweise versucht, mit Java-Script-basierten Anzeigen den ahnungslosen Anwender zum Kauf gefälschter Antivirensoftware zu verleiten. Und spezielle Malware kapert ganze Browsersessions, indem sie DNS-Adressen manipuliert. Das Ziel: Identitätsdiebstahl oder das Ausspähen von Anmeldedaten und Transaktionsnummern für Online-Banking.

Nach wie vor haben Apple-Systeme den Nimbus, dass sie immun sind gegen alle Arten von digitalen Bedrohungen. Dabei vergessen viele Anwender, dass die Einführung von Applikationen anderer Hersteller, bspw. Adobe Reader, Mozilla Firefox, aber auch von proprietärer Software wie Apple QuickTime (nicht zu vergessen die Veröffentlichung von JavaScript und Web 2.0-Applikationen für Safari und Firefox), zahlreiche Sicherheitslücken im System aufreißt, die als sogenannte Zero-Day-Exploits von Cyberkriminellen für Angriffe auf Apple-Computer genutzt werden.

Spam und Phishing sind die häufigsten Bedrohungen, denen Mac-Anwender ausgesetzt sind. Denn diese Form von Angriffen ist plattform- bzw. betriebssystemunabhängig und adressiert jeden, der einen E-Mail-Dienst nutzt. E-Mail-Accounts, die nicht durch Spam- und Phishingfilter geschützt werden, gelten als eine der häufigsten Ursache für den Verlust von persönlichen oder geschäftlichen Daten.

Da Macintosh-Systeme auf der bekannten Intel-Technologie basieren, ist es relativ einfach, mittels Boot Camp oder einer Vitalisierungs-Software wie Parallels Desktop, VMware Fusion oder Virtual Box auch andere Betriebssysteme, zum Beispiel Microsoft Windows, auf Apple-Computern zu installieren. Was viele Anwender solcher Multi-Boot-Konfiguration gar nicht ahnen: Ihre Windowsinstallation kann durch Viren und Würmer infiziert werden, sofern keine geeignete Sicherheitslösung verwendet wird.

Im direkten Vergleich mit Windows-Usern, die Tag für Tag ein wahres Bombardement von digitalen Schädlingen abwehren müssen, leben Macintosh-User diesbezüglich relativ unbeschwert. Trotzdem sollten auch sie präventiv ihren Computer schützen, um sorgenfrei im Internet zu surfen.

## BitDefender Antivirus for MAC OS X

Schon früh hat BitDefender auf Bedrohungen für Apple-Systeme reagiert und bietet bspw. mit Antivirus für Mac OS X eine zuverlässige Schutzlösung für Macintosh Computer. Die Software basiert auf der mehrfach ausgezeichneten BitDefender-Antivirus-Technologie und bietet Schutz gegen spezialisierte Macintosh-Viren und blockt E-Threats, die Windows attackieren.