PANDA SECURITY | *The Cloud Security Company*

INHALT

“Mac OS X ist eine sichere Plattform, weil Windows-Viren sie nicht angreifen”

GIBT ES SICHERHEITS-PROBLEME BEI MAC OS X?

IT-Sicherheitsforen sind häufig voll von Kommentaren, die Apple-User hinsichtlich der Sicherheit beruhigen sollen. Sollten Sie sich trotzdem um die Sicherheit Ihres Mac OS-X Systems sorgen? Auf jeden Fall! Wenn Sie über bestimmte Ereignisse nachdenken, die seit Ende 2011 aufgetreten sind, kämen Sie zur selben Schlussfolgerung. Lassen Sie sich also nicht von vermeintlichen „Experten“ in Sicherheit wiegen. Denn diese werden die Folgen ihrer unklugen Ratschläge nicht selber tragen müssen.

Es gibt keine offiziellen Diskussionen über das Sicherheitskonzept in Apple-Systemen. Woran liegt das? Es stimmt, dass Apple in der Vergangenheit nur wenige Sicherheitsprobleme hatte. Aber das ist hauptsächlich das Ergebnis geringerer Marktanteile im Vergleich zum direkten Mitbewerber Windows.

Die Wahrheit ist, dass es Hackern nichts eingebracht hätte, für so eine Nischenplattform Malware zu entwickeln. Warum hätte also Apple Maßnahmen zum Schutz seiner Kunden ergreifen sollen, wenn diese in der Vergangenheit keiner akuten Gefährdung ausgesetzt waren? **Mit einem globalen Anteil am Desktop-Markt von ca. 6 % im Jahre 2012 hat es sich weder gelohnt, Malware für Mac zu entwickeln, noch war es rentabel, das Apple Betriebssystem gegen etwas zu verteidigen, das kaum existierte.**

Der Sicherheitshinweis, der in der Vergangenheit auf Apples Webseite erschien, war eindeutig.

Er bekommt keine PC-Viren

"Ein Mac ist nicht anfällig für die Tausenden von Viren, die Windows-basierte Computer plagen. Das ist so dank der in Mac OS X eingebauten Sicherheitsmaßnahmen, die Sie schützen, ohne dass Sie etwas dafür tun müssen."

Schützen Sie Ihre Daten. Ohne etwas dafür zu tun.

"Ohne dass Sie etwas dafür tun müssen, schützt OS X vor Viren und anderen schädlichen Anwendungen oder Malware. Zum Beispiel verhindert es Aktivitäten von Hackern durch die sogenannte „Sandboxing"-Technik – sie legt fest, welche Aktionen die Programme auf Ihrem Mac ausführen, auf welche Dateien sie zugreifen und welche anderen Programme sie öffnen können."

Apple beschreibt PC-Viren als das einzige potenzielle Problem und spricht über Sicherheitsmaßnahmen, die ins Betriebssystem eingebaut sind, um die Plattform zu schützen; eine Plattform, die angeblich so sicher ist, dass die User absolut nichts zu ihrem Schutz unternehmen müssen. Eine originäre Sicherheitslücke existierte – vermeintlich – nicht.

Doch im Juni 2012 änderte sich diese Aussage merklich.

Er wurde gebaut, um sicher zu sein

"Ins OS X eingebaute Sicherheitsmaßnahmen schützen Sie vor unbemerktem Download von Schadsoftware auf Ihren Mac."

Sicherheit. Direkt eingebaut

"OS X wurde mit leistungsstarken, fortschrittlichen Technologien entwickelt, die hart arbeiten, um Ihren Mac zu schützen. Zum Beispiel verhindern sie Aktivitäten von Hackern durch die sogenannte „Sandboxing"-Technik – sie legt fest, welche Aktionen die Programme auf Ihrem Mac ausführen, auf welche Dateien sie zugreifen und welche anderen Programme sie öffnen können."

Von nun an wurden PC-Viren nicht mehr erwähnt. Und man kann sich leicht vorstellen, warum. Es war nicht länger möglich, die Existenz von spezieller Malware für Mac zu ignorieren. Um auf der sicheren Seite zu sein, zog Apple auch die Aufforderung zurück, dass User nichts tun sollten, um ihre Systeme zu schützen.

Im Juni 2012 sprach Apple zum ersten Mal in einer Grundsatzrede auf der WWDC (weltweite Entwicklerkonferenz) über Malware, und zwar im Rahmen der Präsentation seiner Gatekeeper-Technologie, welche dabei „helfen würde, das System malwarefrei zu halten". All dies zeigt, dass Apple-Plattformen schon immer anfällig für Malware gewesen sind, genauso wie die Systeme seiner Mitbewerber.

Das wurde schließlich gegen Ende des Jahres 2011 bewiesen, als ein Apple-Sicherheitsprovider – Intego – einen Trojaner identifizierte, den er „Flashback" nannte. Diese Malware nutzte eine Schwachstelle in Java aus, die seit mehreren Wochen bekannt gewesen war. Im Laufe mehrerer Monate wurden mehr als 600.000 Macs infiziert. Zu Apples Leidwesen befanden sich 274 dieser Systeme in Cupertino (Kalifornien), dem Hauptsitz von Apple.

Jeder erfahrene Windows-User weiß, dass viele Infektionen ziemlich offensichtlich sind und oft zu Veränderungen am System führen, die auf das Vorhandensein von Malware auf dem Computer hindeuten können. Bei einer Mac-Plattform könnte man jedoch schon eine ganze Weile infiziert sein und es nicht bemerken, da Mac OS X ein falsches Gefühl der Sicherheit vermittelt. Das ist jedoch äußerst schädlich für die Sicherheit Ihrer Daten.

Apple-Plattformen sind schon immer anfällig für Malware gewesen, genauso wie die Systeme der Mitbewerber.

“Es gibt keine Mac OS X Viren”

STIMMT ES, DASS ES KEINE VIREN FÜR MAC GIBT?

Gespräche über Sicherheit in Mac-Umgebungen findet praktisch nicht statt. Denn damit begibt man sich auf der Gebiet der „Fehler und Mängel“ und kommt zwangsläufig zum Thema „Markentreue“. Sicherheitsexperten sind der Meinung, dass „die größte Schwachstelle bei Macintosh der Glaube der Fans ist, dass Apple-Betriebssysteme überlegen und deshalb immun gegenüber Malware sind.“

Genaugenommen ist ein Virus ein Schadprogramm, das in ein anderes Programm oder in eine Datei eingebettet ist und sich selbst auf anderen Computern verbreiten kann. Flashback war jedoch kein Virus, sondern ein Trojaner. Nach seiner Installation lud er speziell entwickelte Software zum Diebstahl von Bankinformationen, Passwörtern und anderen vertraulichen Daten des Users herunter. Deshalb sollten wir über Malware und Sicherheit im Allgemeinen sprechen und nicht nur über Viren.

Zu behaupten, dass es keine Viren für Mac-Systeme gäbe, ist äußerst gefährlich: Es führt zu Verwirrung. Und in Bezug auf Sicherheit führt Verwirrung zu finanziellen Verlusten.

Abgesehen von Flashback gibt es weitere Malware-Exemplare für Mac, die Auswirkungen hatten:

Pintsized

Dies ist eine Malware, die Schwachstellen in Java ausnutzt, um auf dem Computer eine Hintertür zu öffnen. Durch diese kann ein Hacker die Fernkontrolle des Systems übernehmen.

CoinThief

Diese Malware gibt vor, eine legitime App für Zahlungen im Internet zu sein, aber in Wirklichkeit stiehlt sie Bitcoins.

Icefog

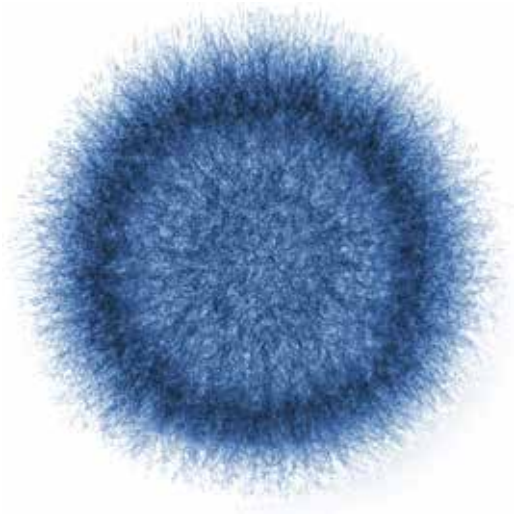
Hierbei handelt es sich um eine plattformübergreifende Malware, die bei der Cyber-Spionage in Japan, Südkorea und anderen Teilen Asiens genutzt wurde.

Mac Defender

Diese gefälschte Antivirenlösung fordert die User auf, das Programm zu registrieren und für den „Schutz“ zu zahlen.

Die Auswirkungen von Malware sind immer dieselben, egal ob es sich dabei um Viren, Trojaner, Rootkits oder Ransomware handelt. Es ist nicht nötig, den gesamten technischen Fachjargon zu kennen. **Sie müssen nur wissen, dass es da draußen Malware gibt, die Ihr Mac OS X betreffen KANN und dass es Ihr Geld ist, das auf dem Spiel steht.**

Zu behaupten, es gäbe keine Viren, die Mac-Systeme betreffen, ist äußerst gefährlich: Die größte Schwachstelle von Macintosh ist der Glaube der Fans, dass das Apple-Betriebssystem überlegen und deshalb immun gegenüber Malware ist.



“Sie müssen sich nicht um die Sicherheit Ihres Macs sorgen”

WAS TUT APPLE, UM DIE USER ZU SCHÜTZEN?

Auch wenn es immer noch einige User leugnen: es herrscht Cyberkrieg. Das zeigt sich daran, dass ständig Angriffsszenarien und Verteidigungsmaßnahmen entwickelt werden. Es gibt eine Gemeinschaft, deren finanzielle Motivation, Malware zu entwickeln, parallel zu den Verkaufszahlen von Mac OS X wächst. Folglich entwickelt Apple Schutz- und Verteidigungsmaßnahmen, um die User zu schützen… so scheint es zumindest.

Das Hauptproblem ist, dass Apple sehr spät auf dem Cyber-Schlachtfeld erschienen ist; einem Schlachtfeld, auf dem Microsoft bereits kampferfahren ist. Mit der Entstehung des Internets gab es einen exponentiellen Zuwachs bei Malware. Windows 95, 2000 und XP waren die Plattformen, die stark angegriffen wurden und aufgrund derer Microsoft – praktisch allein – mit der Situation fertig werden musste. Es hat nie zuvor eine ähnliche Situation gegeben und das Unternehmen musste unter dem Druck von Millionen infizierter Systeme schnell reagieren.

Das Ergebnis solch einer steilen Lernkurve ist ein Unternehmen, das sich sehr für Sicherheit engagiert. Es hat einen klaren Zeitplan für die Veröffentlichung von Sicherheitsreports sowie die Kapazität, schnell Patches und Updates für sein Betriebssystem herauszubringen.

Bei Apple ist es genau das Gegenteil: Apple veröffentlicht Updates nur, wenn das für **notwendig erachtet wird. Im Fall von Flashback dauerte es sechs Wochen bis zur Beseitigung der Schwachstellen, die zur Infektion führten.** Und das, obwohl Oracle bereits Patches entwickelt und veröffentlicht hatte.

Es gab ähnliche Fälle, wie z. B. Icefog, wo **Apple zwei Wochen brauchte,** um die Signaturdatei in sein Antivirenprogramm Xprotect zu integrieren. In dieser Zeit infizierte Icefog weiterhin Computer von Usern, die sich des Problems nicht bewusst waren. **Vergleichen Sie das mit Anbietern von Cloud Security, die Updates in wenigen Minuten bereitstellen!**

Apple hat auch keine klaren Richtlinien, wenn es darum geht, das Ende von Produkt-Support bekanntzugeben: Bei der Veröffentlichung der Versionen 10.9 und 10.9.1 waren beispielsweise mehrere der enthaltenen Fixes nicht für frühere Versionen erhältlich (Lion und Mountain Lion). Mit dem Erscheinen der Version 10.9.2 veröffentlichte das Unternehmen Fixes, um die User von Lion und Mountain Lion vor Malware zu schützen. Doch diesmal wurde Snow Leopard (10.6) nicht berücksichtigt.

Sollten Sie ein 10.6 System haben, updaten Sie es so bald wie möglich!

Die Konsequenz aus all dem ist, dass **User nicht wissen, wann oder ob es Lösungen geben wird, wenn sie nicht die neueste Version des Betriebssystems haben.**

Mac OS X Sicherheitslösungen erscheinen nach und nach, was eine enorme Verbesserung im Hinblick auf die Sicherheit der Plattform ist. Doch da diese Sicherheitslösungen Teil der Basisinstallation des Apple Betriebssystems sind, wissen Malware-Autoren bereits von der Existenz dieser Sicherheitserweiterungen.

Andererseits hat Apple seit 2009 schrittweise wesentliche Veränderungen in sein Betriebssystem integriert, um die Sicherheit zu stärken. Eine kurze Zusammenfassung könnte Folgendes enthalten:

- **Leopard (10.5)**
  SandBox, Dateiquarantäne und Application Firewall.
- **Snow Leopard (10.6)**
  Antivirenlösung Xprotect.
- **Mountain Lion (10.7)**
  Gatekeeper.

Apple hat schrittweise wesentliche Veränderungen in sein Betriebssystem integriert, um die Sicherheit zu stärken.

Mac OS X Sicherheitslösungen tauchen auf, als wären sie Bioorganismen. Obwohl dies eine große Verbesserung im Hinblick auf die Sicherheit der Plattform ist, hat es denselben Effekt wie die Security Essentials bei Windows. Da sie Teil der Basisinstallation des Apple Betriebssystems sind, wissen Malware-Autoren bereits von der Existenz dieser Sicherheitserweiterungen. So können sie sich auf die Entwicklung von Gegenmaßnahmen konzentrieren, um die Schutzmaßnahmen zu umgehen.

Deshalb sollten User die Basisschutzmaßnahmen von Apple mit guten Antivirenlösungen von Drittanbietern ergänzen.

WAS KANN MAN TUN, UM DAS INFEKTIONSRISIKO ZU MINIMIEREN?

Gesunder Menschenverstand und Vorsicht sind die Eckpunkte bei der Vermeidung von Infektionen. Wir sollten wissen, dass unser System gefährdet ist, und umsichtig bei der Sicherung unserer Daten sein. Außerdem sollten wir ein gutes Antivirenprogramm installieren und ständig updaten sowie verdächtige Dateien blockieren.

Im Jahre 2011 verkündete Apple stolz auf seiner Webseite, dass sein System gegenüber PC-Viren immun sei. Das traf auch mehr oder weniger zu: Im Allgemeinen funktioniert ein Virus, der für ein Windows-System geschrieben wurde, nicht auf einem Mac OS X.

Mit dem Erscheinen von spezieller Malware für Mac OS X waren Bedrohungen für Windows immer noch eine potenzielle Quelle für Probleme in gemischten Umgebungen oder sogar im Hinblick auf das Firmenimage. Stellen Sie sich vor, Sie senden einem Kunden ein Angebot und der Anhang ist mit PC-Viren infiziert. Statistiken von Drittanbietern behaupten, dass 43 % der Malware auf Mac OS X ursprünglich Malware für Windows gewesen sei.

Ob es nun darum geht, Ihre eigenen Systeme, die Windows-Computer in Ihrer Umgebung oder Ihr Firmenimage zu schützen, Sie können Ihrem Mac OS X System mit ein paar einfachen Maßnahmen einen vernünftigen Schutz geben:

Facebook und andere soziale Netzwerke werden sehr oft für die Verbreitung von Malware genutzt.

Bearbeiten Sie nur Dateien aus zuverlässigen Quellen.

1. Ihr Mac-System ist nicht unverwundbar

Bedenken Sie Folgendes: Ihr Mac-System ist nicht unverwundbar. Ihr Computer könnte infiziert sein. Und Ihre Systeme könnten gegen Sie arbeiten, statt Ihnen zu helfen, die Viren zu entdecken. Sie sollten sich besser nicht darauf verlassen, dass Viren auf einem Mac „nicht funktionieren".

2. Kaufen Sie einen guten Virenschutz von Drittanbietern

Egal welche Version von Mac OS Sie haben, ein zusätzlicher Schutz ist sinnvoll. Die Malware, die sich derzeit im Umlauf befindet, hat das Ziel, Apples eigene Schutzmaßnahmen zu überwinden. Je mehr Antivirenlösungen auf dem Markt sind, desto mehr werden die Bemühungen der Hacker geschwächt. Dadurch ist das Risiko einer Infektion viel geringer, als wenn es de facto ein Sicherheitsmonopol gäbe.

3. Installieren Sie alle Updates

Installieren Sie alle Updates für Ihr Betriebssystem und für Anwendungen von Drittanbietern, sobald diese erscheinen.

4. Achten Sie darauf, welche Dateien Sie ausführen

Über Webseiten sozialer Netzwerke wie beispielsweise Facebook erhält man Malware von sogenannten „Freunden". Auch E-Mail-Anhänge von unbekannten Absendern und von P2P-Programmen heruntergeladene Dateien können Malware enthalten. Deshalb sollten Sie nur Dateien von zuverlässigen Quellen herunterladen und ausführen.

5. Deaktivieren Sie problematische Software

Java und Flash sind beides Technologien mit einer ganzen Reihe von Bugs und Schwachstellen. Je nachdem, welche Browserversion Sie haben, deaktivieren Sie das Java-Modul direkt in Ihrem Safari-Browser oder über das Menü „Webseiteneinstellungen verwalten".