

---

IT-Sicherheit bei Apple und Microsoft

## Mythos entzaubert

**Apple rückt Sicherheitslücken weniger konsequent zu Leibe als Microsoft. Das zeigten die ETH-Forscher Stefan Frei, Bernhard Tellenbach und Bernhard Plattner an der jüngsten Black Hat-Konferenz in Amsterdam. Ein Dämpfer für Mac-Fans.**



Mac-Userinnen und -User wännen sich mit ihrem Betriebssystem auf der sicheren Seite, obwohl Apple beim Vergleich mit Microsoft punkte Sicherheitspatches abfällt.

nach Bekanntwerden einer Sicherheitslücke bereit gestellt wurden. Die Forscher griffen für ihre Auswertung auf unabhängige Daten von verschiedenen Quellen, wie The Open Source Vulnerability Database (OSVDB) oder National Vulnerability Database (NVD) zurück. Die Daten decken die letzten sechs Jahre ab.

Die drei ETH-Forscher von der Communication Systems Group haben eine neue Messmethode entwickelt, mit der sie beurteilen können, wie rasch die grossen Softwarehersteller Sicherheitslücken von Betriebssystemen schliessen. Als Mass führen die Forscher die Zero-Day-Patch-Rate ein. Diese beschreibt, wie oft die Hersteller unmittelbar nach öffentlichem Bekanntwerden einer Sicherheitslücke einen Patch zur Verfügung stellen können. Neben der Zero-Day-Patch-Rate werteten sie auch aus, wie oft Patches 30, 90 und 180 Tage

### Mehr Flicker für Microsoft

Die Resultate der Studie zeigen: Microsoft hat bei Sicherheitsbelangen die Nase vorn. In den untersuchten sechs Jahren gab es bei Microsoft durchschnittlich deutlich weniger als 20 ungepatchte Sicherheitslücken pro Tag, bei Apple jedoch deutlich mehr als 20. Die Autoren haben sogar beobachtet, dass sich die Situation bei Apple ab 2006 verschlechtert hat. Die Firma konnte zudem erst ab Mitte 2003 Zero-Day-Patches ausliefern.

Die Daten zeigen den ETH-Forschern aber auch, dass die Sicherheitsleistungen beider Softwarehersteller in den Jahren 2004 und 2005 stark zurückgingen. Das habe möglicherweise damit zu tun, dass Hacker neue Techniken wie das Fuzzing einsetzten, auf welche die beiden Hersteller noch nicht vorbereitet gewesen seien. "Es braucht immer Zeit, bis sich die Hersteller auf neue Hackertools und Methoden einstellen", betont Frei.

Die Zero-Day Patch-Rate scheint zeitlich mit dem Release neuer grosser Softwarepakete, wie Betriebssystemen und Service-Packs, zu korrelieren. Jeweils ein halbes Jahr vor dem Release neuer grosser Softwarepakete fällt sie deutlich ab. Das könnte damit zu tun haben, dass die Ressourcen an Programmierern für neue Produkte benötigt werden und weniger für das Erstellen von Patches zur Verfügung stehen.

## Mythos wankt

Die ETH-Studie kratzt am Mythos, dass die Produkte aus dem Hause von Steve Jobs sicherer sind als diejenigen aus der Küche von Bill Gates. "Fachleuten war dieses Entwicklung seit längerem bekannt", sagt Frei, "wir haben nun aber zum ersten Mal empirische Daten dazu gesammelt."

Microsoft ist aufgrund der grösseren Verbreitung schon viel länger mit Sicherheitsproblemen konfrontiert. "Microsoft hat daraus aber viel gelernt", bilanziert Frei. Der Dauerbeschuss habe dazu geführt, dass der Softwaregigant in den vergangenen Jahren einen guten Kontakt zur Security-Community aufgebaut hat, offen mit ihnen kommuniziert und die Mühe nicht scheut, die Schwachstellen zu beheben. Anders Apple, deren Kommunikation mit der Security-Community in diesem Bereich offenbar schlecht ist. "Apple hat die Prioritäten anders gesetzt", sagt er.

Für ihre Arbeit haben die IT-Wissenschaftler nur diejenigen Schwachstellen ausgewertet, die von den Herstellern auch gepatcht wurden. Sicherheitslücken, welche die Software-Firmen selbst entdecken und beheben, kommen in der Regel gar nicht erst ans Tageslicht. "Darüber sind leider keine öffentlichen Daten vorhanden", sagt Frei.

## Weitere Firmen unter Lupe nehmen

Die ETH-Forscher wollen als nächstes weitere Software-Hersteller unter die Lupe nehmen, wie zum Beispiel Oracle und Red Hat / Linux. Diese direkt mit Apple und Microsoft zu vergleichen, hätte jedoch wenig Sinn ergeben, findet Frei. "Man muss schon Birnen mit Birnen vergleichen." Es sei in dieser Studie nicht darum gegangen, die beiden Grossen gegeneinander auszuspielen, der Vergleich sei aber interessant und er warte gespannt darauf, wie sich die Zero-Day-Patch-Rate in den nächsten zehn Jahren entwickeln werde.

## Black Hat: Alles um IT-Sicherheit

Viermal pro Jahr findet in Europa, Japan und den USA die so genannte Black Hat-Konferenz statt, an denen sich IT-Sicherheitsexperten, Hacker, Firmenvertreter und Wissenschaftler gleichermassen treffen. An erster Stelle steht der Austausch über die neusten Entwicklungen in der IT-Sicherheit. Im Rahmen der jüngsten Konferenz Ende März in Amsterdam referierten die ETH-Forscher über die Resultate ihrer neuen Studie. Die nächste Konferenz findet Anfang August in Las Vegas statt.

## Referenzen:

Frei, Stefan, Bernhard Tellenbach and Bernhard Plattner (2008): 0-day-patch exposing vendors (in)security performance, <http://www.techzoom.net/risk/>

## Leserkommentare:

Autor: Peter Rüegg | Veröffentlicht: 03.04.08