Black Hat: Neue Metrik für Sicherheit von Betriebssystemen vorgestellt

[28.03.2008 10:12]

Forscher der ETH Zürich haben auf der derzeit in Amsterdam stattfindenden **Black-Hat-Sicherheitskonferenz[1]** ein neues Modell zur Ermittlung der Sicherheit von Betriebsystemen entwickelt. Dazu zählen sie nicht allein die Anzahl der Lücken und wie kritisch diese sind, sondern ermitteln zudem die von ihnen so genannte Zero-Day-Patch-Rate. Diese gibt an, inwieweit ein Hersteller in der Lage ist, zum Zeitpunkt des Bekanntwerdens einer Lücke einen Patch zur Verfügung zu stellen. Um dabei von den Angaben der Hersteller unabhängig zu werden, greifen sie auf zahlreiche unabhängige Quellen zurück wie Secunia, Milw0rm, The Open Source Vulnerability Database (OSVDB), National Vulnerability Database (NVD), CVE und diverse andere.

In ihrem Dokument **"0-Day Patch -Exposing Vendors (In)Security Performance"[2]** (PDF-Datei) führen Stefan Frei, Bernard Tellenbach und Bernhard Plattner von der Communications Systems Group der ETH ihre Methode exemplarisch anhand von Microsofts und Apples Betriebssystemen vor. Als Zeitraum ihrer Bewertung legten sie die letzten sechs Jahre zugrunde. Neben der Zero-Day-Patch-Rate haben die Autoren auch noch die Verfügbarkeit von Patches 30, 90 und 180 Tage nach dem Bekanntwerden der Lücke in ihre Grafiken aufgenommen. Sowohl bei Microsoft als auch bei Apple zeigt sich, dass die Dauer der Bereitstellung eines Patches wuchs, je näher die Veröffentlichung einer neuen Version eines Betriebssystems oder eines Service Pack rückte. Offenbar bindet dies erhebliche Ressourcen, die dann nicht mehr der Patch-Entwicklung zur Verfügung stehen.

Die Forscher kommen darüber hinaus zu dem Ergebnis, dass die Zahl der offenen Lücke sich bei Microsoft mittlerweile stabilisiert habe. Bei Apple zeige sich allerdings der gegenteilige Trend, wobei Apple Microsoft sogar bereits überholt habe und im Schnitt mehr offene Lücken aufweise. Die Ergebnisse ihre Untersuchung würden die allgemeine Annahme, dass Apple von Natur aus sicherer sei, nicht bestätigen. Das **letzte Update von Apple[3]** für Mac OS X beseitigte 46 Lücken, dazu kamen noch 13 allein für den Browser Safari.

Siehe dazu auch:

- **0-Day Patch -Exposing Vendors (In)Security Performance[4]**, Studie von Stefan Frei, Bernard Tellenbach und Bernhard Plattner

(**dab[5]**/c't)

URL dieses Artikels:
http://www.heise.de/security/news/meldung/105644

Links in diesem Artikel:
[1] http://www.blackhat.com/html/bh-europe-08/bh-eu-08-speakers.html#Frei
[2] http://www.techzoom.net/papers/blackhat_0day_patch_2008.pdf
[3] http://www.heise.de/security/Apple-Sicherheitsupdate-behebt-46-Fehler--/news/meldung/105283
[4] http://www.techzoom.net/papers/blackhat_0day_patch_2008.pdf
[5] mailto:dab@ct.heise.de