2014
23
Okt
Botnetze breiten sich aus
Ein kürzlich entdecktes Botnetz für DDoS-Angriffe breitet sich nach Angaben von Experten ungehemmt aus. Inzwischen seien auch Windows, Linux un Mac OS X -Server gefährdet. Der Zweck der darüber gefahrenen Angriffe bleibt unklar jedoch Abhilfe ist einfach möglich.
Die Schadsoftware nutzt eine vor Monaten geschlossene Java-Lücke aus um ein Botnetz aufzubauen. Als Schutz dagegen reicht der Umstieg auf eine aktuelle Version von Java 7 aus, die <u>Oracle</u> für viele Betriebssysteme kostenlos bereitstellt. Mac-Anwender bekommen auch für das ältere Java 6 noch eine korrigierte Version für <u>OS X 10.6</u> sowie <u>10.7 und später</u> bei Apple.
Was ist ein Botnetz?
Ein Botnetz ist ein großer Zusammenschluss von mit Malware infizierten Rechnern. Diese stellen auf Wunsch des Botnetz - Betreibers genug Rechenkapazitäten zur Verfügung, um Programme zu kompilieren, oder setzen eine Webseite durch eine Flut von Aufrufen außer Betrieb. Diese sogenannten DDos-Attacken gehen oft nicht vom Betreiber der Botnetze aus, sondern werden von Kunden gekauft.
2014
16
Mai
NSA manipuliert Router beim Export aus den USA

Bereits vor einigen Monaten hatte Netzaktivist Jacob Appelbaum die Behauptung aufgestellt, dass der US-Geheimdienst NSA Router beim Export aus den USA manipuliert und mit eigener Spyware versieht. In seinem Buch "Die globale Überwachung" greift Journalist <u>Glenn Greenwald</u> dieses Thema erneut auf, und liefert dafür auch gleich die passenden Beweise.

Weiterlesen NSA manipuliert Router beim Export aus den USA
2014
09
Apr
Heartbleed-Bug
Sicherheitshinweise zum Heartbleed-Bug
Eine Sicherheitslücke in der Software OpenSSL sorgte in den letzten Tagen für Unsicherheit. Der sogenannte Heartbleed-Bug ermöglicht es Angreifern, sensible Daten aus dem Speicher eines Servers auszulesen. Die terralink networks hat sofort Gegenmaßnahmen ergriffen und auf allen Systemen den OpenSSL Patch ausgerollt sowie die eigenen Zertifikate ersetzt.
Weiterlesen Heartbleed-Bug
2014