Erledigt El Capitan und die System Integrity Protection - Was ist das und wie kann ich es ändern?

Beitrag von „griven“ vom 31. Oktober 2015, 23:19

QSchneider: beide Artikel sind interessant und fassen die Problematik ziemlich gut zusammen. Tatsächlich hat PikerAlpha vollkommen recht damit, dass es eine dumme Idee ist OS-X ohne aktivierte SIP zu betreiben denn schließlich dient dieses mächtige Werkzeug dazu das System vor äusseren Einflüssen zu schützen und das auf eine äusserst effektive Weise. Es gibt eigentlich auch gar keinen Grund die SIP abzuschalten bzw. im Falle eines Hackintoshes abgeschaltet zu lassen nachdem das System fertig installiert wurde denn von diesem Zeitpunkt an ist es eigentlich nicht mehr erforderlich irgendetwas an den Systemverzeichnissen zu verändern. Daher von mir die klare Empfehlung die SIP zu aktivieren sobald das System fertig installiert ist und auch aktiviert lassen es sei denn es muss nach einem Update zum Beispiel etwa die AppleHDA neu installiert werden. Interessanter in dem Zusammenhang ist auch der Artikel zum umgehen des Signaturzwangs für Extensions. Auf echten MAC´s sicher kein wirkliches Problem da hier eben nur der Apple eigene OS Loader zum Einsatz kommt und dieser wird den prelinked Kernel (KernelCache) nicht verändern anders sieht es aber auf Hackintoshes aus und für die ist diese Erkenntnis eher Segen als Fluch denn so wird es möglich das System mit minimalen Veränderungen an den SystemFiles zu starten was für uns nur gut ist. Ob hieraus ein Sicherheitsrisiko erwachsen mag möchte ich nicht abschließend beurteilen denn letztlich muss jeder für sich selbst entscheiden welche extensions aus welchen Quellen er verwendet und welche eben nicht. Eine generelle Angreifbarkeit aufgrund der Tatsache, dass sich dem System unsignierte Extensions unterjubeln lassen möchte ich aber ausschließen denn dazu müsste ein potentieller Angreifer sich die Mühe machen zum einen zu bestimmen welcher Bootloader zum Einsatz kommt und zum anderen auch noch den vermeidlichen Schadcode in den entsrechenden Verzeichnissen unterbringen alles in allem eher unwahrscheinlich.